Aprende cómo administrar la red en un Instituto de Enseñanza Secundaria...

ADMINISTRAR LA RED EN UN IES

ANTECEDENTES.

Nuestro Instituto de Enseñanza Secundaria está formado por unos 30 profesores y 400 alumnos, además de 5 personas que trabajan como Personal Auxiliar de Control.

La oferta educativa comprende las Familias de Sanidad, Servicios a la Comunidad e Informática, y se imparten ciclos formativos de Grado Medio (ESI, Atención sociosanitaria, Farmacia, Enfermería y ciclos formativos de Grado Superior (Educación Infantil, Diagnóstico Clínico, Salud Ambiental).

Esta comunidad educativa realiza tareas diversas, que requieren además de una red de área local, una conexión a Internet .

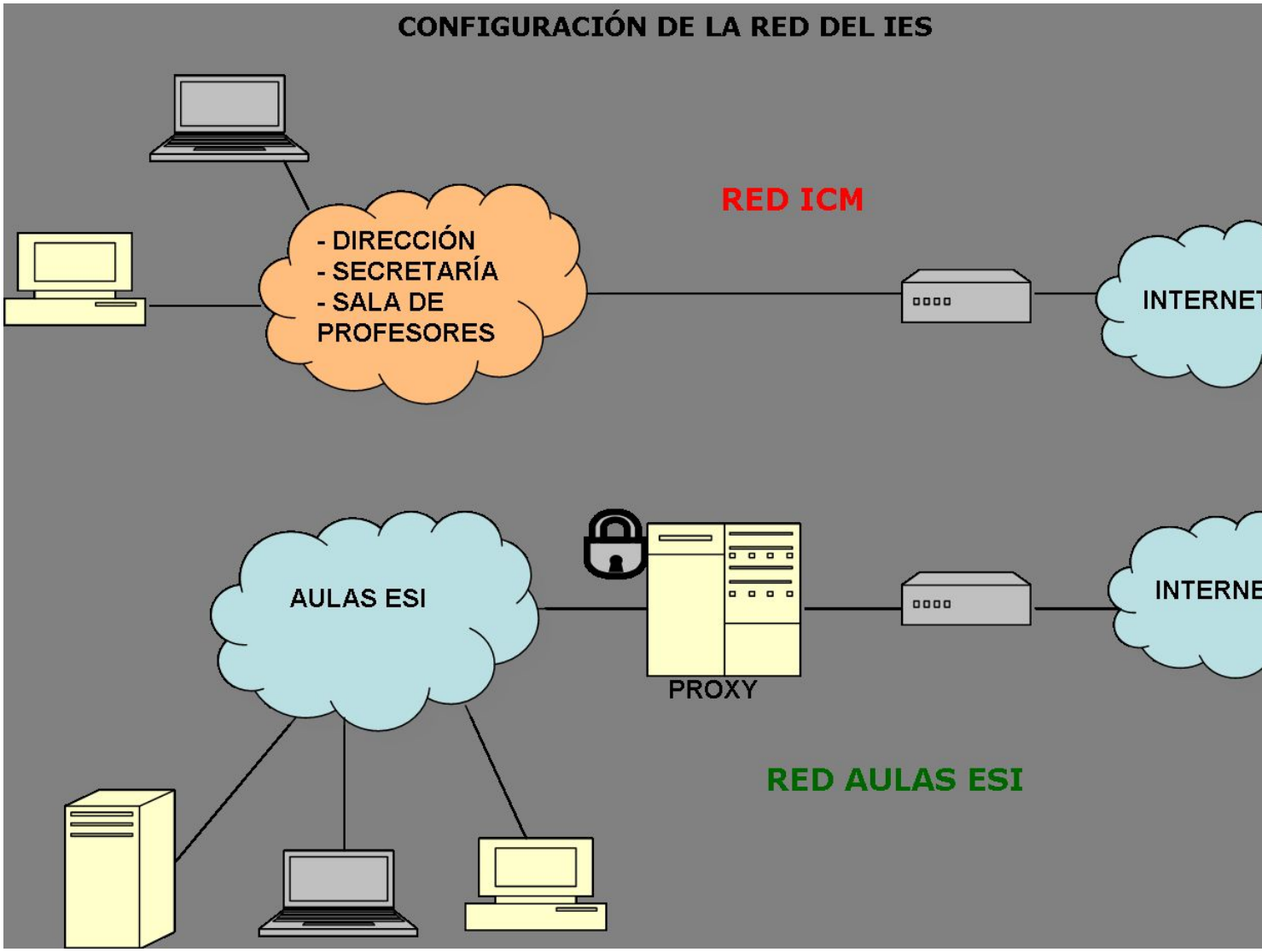
La Comunidad de Madrid provee a los centros de Educación Secundaria de diferentes tipos de instalaciones, en concreto nosotros tenemos dos redes de área local y dos accesos a Internet diferenciados.

En primer lugar tenemos la red ICM[1], que utilizan la Secretaría del Centro, los Órganos de dirección y sala de profesores. Esta red la mantiene por completo el personal de ICM, y el acceso a Internet se realiza a través del proxy 213.4.106.164.

La segunda red es utilizada por las aulas de informática. Tenemos cinco aulas distribuidas en las tres plantas del instituto, con unos 18 equipos cada una. Estos equipos son ordenadores personales y servidores. Cada aula está dotada con un swtich de 10/100 Mbps al que están conectados todos los equipos.

Hemos instalado un filtro utilizando un servidor proxy Squid a través del que pasan los PC's de estas aulas, con el que controlamos las páginas que visitan los alumnos; para ello utilizamos herramientas como Dansguardian y Sarg en las que entraremos en detalle más adelante.

Por otro lado, nuestro ISP o proveedor de servicios de Internet es Telefónica. Utilizamos un router Zyxel y el ancho de banda es de 3 Mb.



NECESIDADES WIFI

Aunque el servicio básico de acceso a Internet está cubierto, es necesario dotar de acceso a Internet (inalámbrico) a los equipos portátiles de los departamentos, personas ajenas al centro que utilicen dispositivos móviles, así como prestar un servicio añadido a los alumnos para utilizar videoconsolas, teléfonos móviles etc..

ESTUDIO PRELIMINAR.

Hacemos un estudio del centro con los alumnos de 1º de ESI.

Trataremos de instalar una red Wifi dando cobertura a la totalidad del IES, poniendo hincapié en algunas zonas comunes del centro como la Biblioteca, la Sala de profesores, Cafetería y parte del patio.

TECNOLOGÍA WIFI.

Wi-Fi (Wireless Fidelity) es una de las tecnologías de comunicación inalámbrica (sin cables - wireless) más extendidas. También se conoce como WLAN o como **IEEE 802.11.**

Los subestándares de Wi-Fi actualmente en el ámbito comercial son:

-

802.11b:

Pionero en 1999.
Opera en la banda de los 2.4 GHz.
Alcanza una velocidad máxima de 11 Mb/sg.

-

802.11g:

Estrenado en 2003, y actualmente el más extendido.

Opera en la banda de los 2.4 Ghz.

Alcanza una velocidad máxima de 54 Mb/sg.

-

802.11n:

Desde 2006 hay productos. Aprobado en Enero de 2008

Opera en la banda de los 2.4 Ghz y 5 Ghz.

Alcanza una velocidad máxima de 300/100 Mb/sg (teóricos/reales)

1. WIFI. CONCETPOS BÁSICOS.

-

Access Point: (Punto de Acceso o AP)

Es el dispositivo físico que hace de *puente* entre la red cableada y la red inalámbrica. Los APs son puentes traductores 802.11 a 802.x (generalmente 802.3)

-

Accesorio Wi-Fi:

Es el accesorio adicional que usaremos para incoporar el estándar 802.11 a nuestro dispositivo móvil, en caso de no tener Wi-Fi integrado.

Estos accesorios pueden encontrarse en formato de tarjetas PCMCIA (para portátil), PCI y USB.

-

SSID: (Service Set Identification) :

Nombre con el que se identifica a una red Wi-Fi. Este identificador viene establecido de fábrica pero puede modificarse a través del panel de administración del Punto de Acceso. Podemos habilitar o deshabilitar su difusión.

-

Canal:

Es una frecuencia de uso único y exclusivo para los clientes dentro de su cobertura.

La frecuencia más usada es la de 2.4 Ghz; esta frecuencia está libre en casi todos los países del mundo.

Los canales que se pueden utilizar varían según el punto geofráfico: América, Europa, Japón

etc.

-

Modos de conexión: Infraestructura y Ad-hoc

Infraestructura

Modo de conexión en una red wireless que define que nuestro equipo (cualquier dispositivo móvil) se conectará a un Punto de Acceso. El modo de conexión deberá de especificarse en la configuración de nuestro equipo o del accesorio Wi-Fi. En redes inalámbricas la asociación a un AP equivale a conectarse por cable a un switch en una red ethernet .

Ad-Hoc: Punto a punto.

Modo de conexión en una red wireless que define que nuestro equipo se conectará directamente a otro equipo, en vez de hacerlo a un Punto de Acceso.

2. ELEGIR ARQUITECTURA.

-

Redes de infraestructura: con al menos un AP. Pueden ser de dos tipos:

-

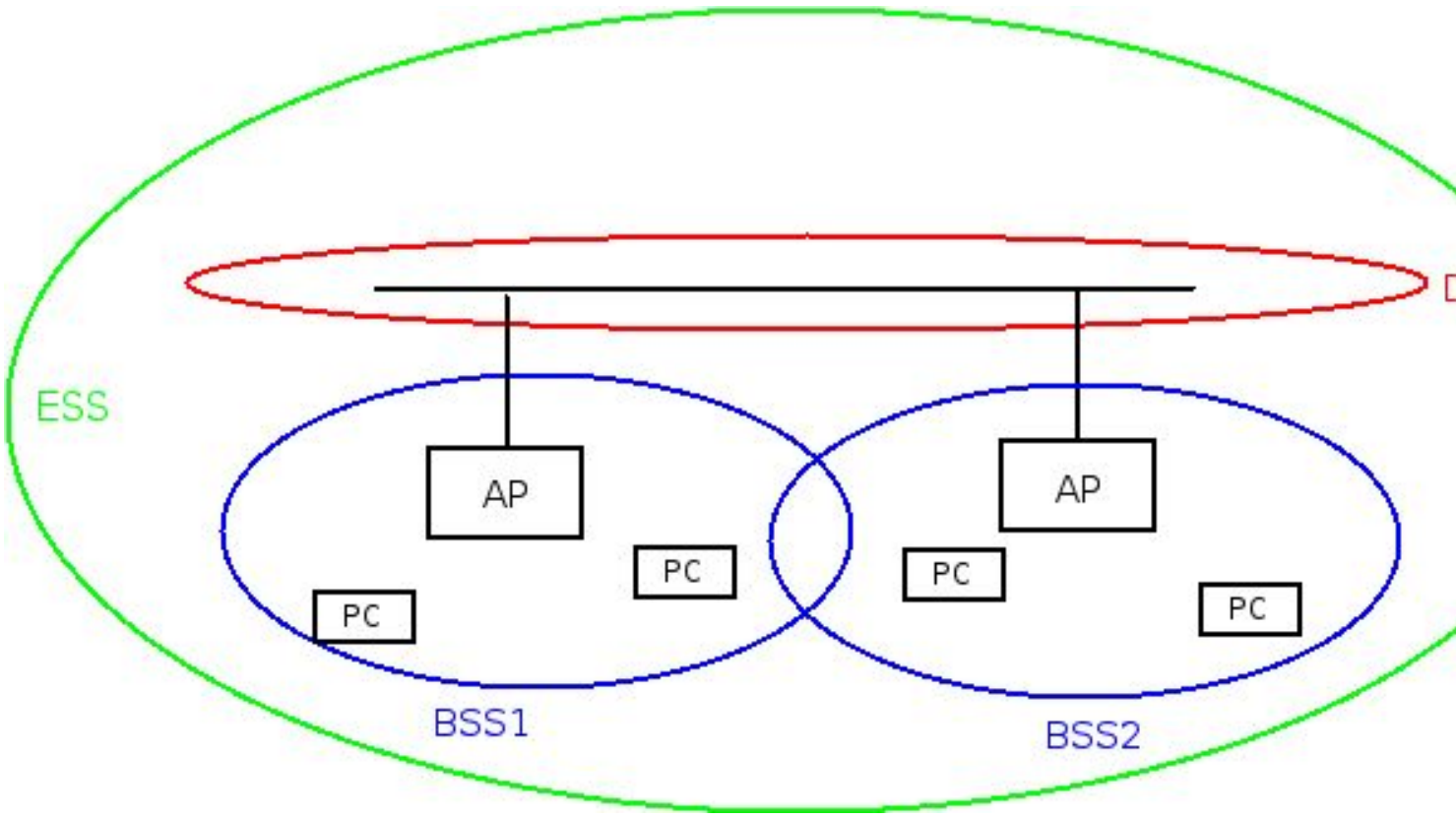
BSS (Basic Service Set): la zona de cobertura que abarca un AP. El AP puede o no, estar conectado a una red .

-

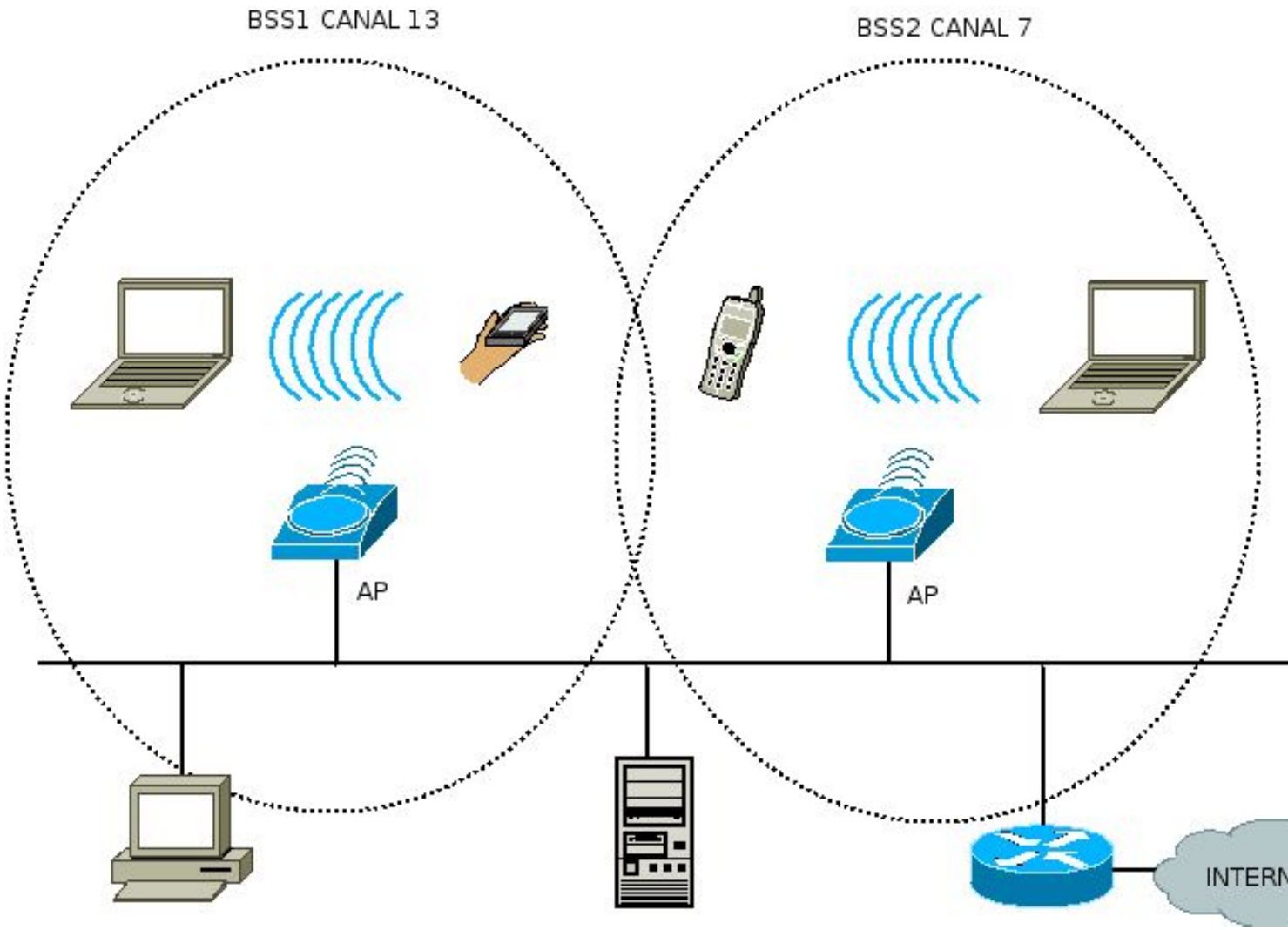
ESS (Extended Service Set): es un conjunto de dos o más BSS, es decir dos o más APs interconectados a nivel 2 OSI . La red que interconecta los APs se denomina el DS (Sistema de distribución). Es decir todos los AP's de la red tendrán idéntico SSID.

-

DS (Distribution System): es el medio de comunicación entre los AP. Normalmente es Ethernet, pero puede ser cualquier medio. Debe haber conectividad a nivel de enlace
2
entre los APs que forman el ESS. En nuestra instalación aprovecharemos el cableado Ethernet para conectar los AP's.



Vamos a utilizar una arquitectura de este tipo



Como vemos, los portátiles, la pda y el móvil están conectados de forma inalámbrica a varios AP's que hemos conectado a la red Ethernet, a través de la cual accedemos a Internet previo paso por el router.

Si movemos uno de estos dispositvos desde el BSS1 al BSS2, se produce lo que se llama itinerancia o roaming.

3. SEGURIDAD, ROAMING Y AUTENTIFICACIÓN

Itinerancia (Roaming):

-

Una estación no puede estar asociada a más de un AP a la vez.

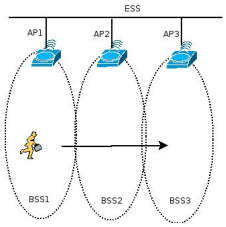
-

Si se aleja de un AP y se acerca a otro deberá reasociarse, es decir desasociarse del primer AP y asociarse al segundo (suponiendo que ambos pertenecen al mismo ESS, es decir tienen el mismo SSID) . Este proceso es transparante para el usuario.

-

Si el proceso se realiza con suficiente rapidez es posible que no se pierdan paquetes. El concepto de "rápido" depende

del grado de solapamiento de las áreas de cobertura de los dos APs y de la velocidad con que se esté moviendo la estación.



Autentificación:

-

Una red inalámbrica sin protección esta muy expuesta a ataques. Para evitarlos se debe utilizar algún protocolo de protección, como WEP[3], WPA[4], Servidor RADIUS[5] etc.

-

Cuando se utiliza protección, la red va a obligar a las estaciones a autentificarse antes de asociarlas.

-

La autentificación se hace antes de asociarse y no se hace al reasociarse.

-

Cuando una estación cambia de AP dentro de un mismo SSID solo tiene que reasociarse, no reautenticarse

- La autentificación se hace con un determinado SSID (en nuestro caso 'villaverde'), la asociación con un determinado BSSID (es la dirección MAC del AP en cuestión).

PRESUPUESTO. ¿QUÉ COMPRAMOS?.

Decidimos comprar 6 AP'S. Desechamos las antenas porque con los AP's habrá suficiente cobertura; podríamos colocar una antena tipo parche para el patio, pero la señal se alejaría demasiado.

Nuestra elección es Wireless-G Broadband Router WRT54GL (54 euros + IVA) con antenas dipolo diversidad, que trabaja como AP y si fuera necesario como router. Además tiene 4 puertos Ethernet.

Con unos 360 euros podemos construir la Wifi.

TRABAJO DE CAMPO. COBERTURA, CANALES Y DISPOSICIÓN DE LOS AP'S.

Las tres plantas del edificio quedan con cobertura, pondremos dos puntos de acceso en cada planta. Elegimos canales que no estén solapados para evitar interferencias.

En Europa se pueden utilizar los canales del 1 al 13 en el rango de frecuencias 2.412-2.484 MHz.

Para no solaparlos podemos elegir 1-5-9-13 ó 1-7-13.

Una vez hecho el diseño es imprescindible un trabajo de campo, para ver si hay zonas sin cobertura o con interferencias, siendo necesario añadir o eliminar AP'S.

-

Dependiendo de la estructura y forma del edificio normalmente en 802.11g cada AP puede dar cobertura a una superficie de 300 a 1000 m2

-

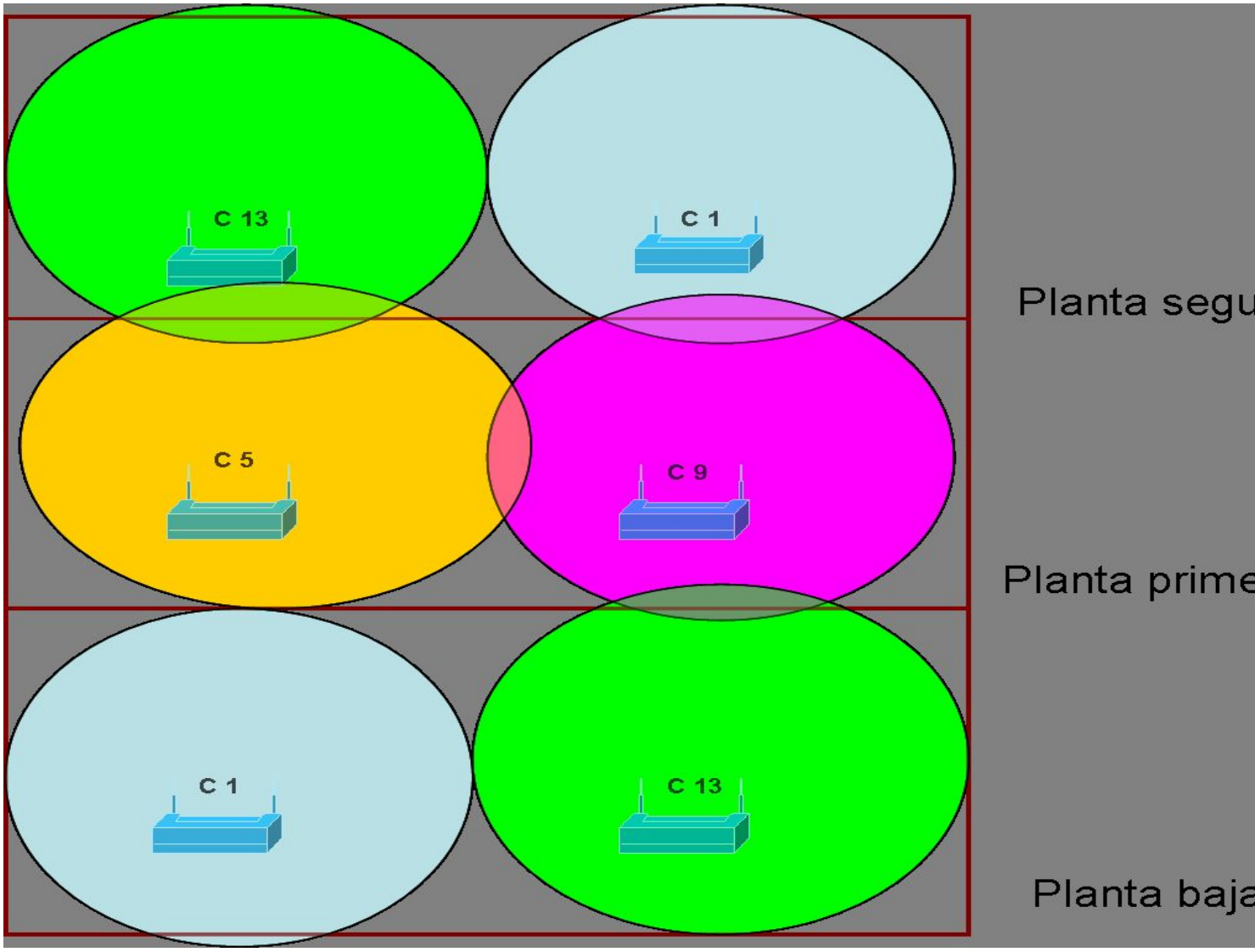
En algunos casos la señal puede atravesar 2-3 paredes, en otros puede cubrir plantas contiguas

-

Si se instala una densidad de AP's excesiva los equipos se interfieren mutuamente. En esos casos es conveniente reducir la potencia de cada AP, si es posible.

-

Si la previsión es de un gran número de usuarios o se quiere dar muho rendimiento interesa que las celdas sean pequeñas. Entonces interesa poner más AP's que los estrictamente necesarios con potencia de emisión reducida (ej. un salón de conferencias)



CONFIGURACIÓN DE LOS AP

Para la configuración del AP debemos conectarlo al PC con un cable de red que proporciona el fabricante (se podría usar un cable de par trenzado normal).

Abrimos un navegador y tecleamos la ip del AP (típicamente http://192.168.1.1). Cada router, dependiendo del fabricante y/o modelo, tiene una ip y usuario/password diferentes; se puede ver en la documentación del producto).

Todos los AP han de tener el mismo SSID (ej. 'villaverde'), le asignamos una IP fija, y cada vez que queramos cambiar la configuración utilizaremos la fija.

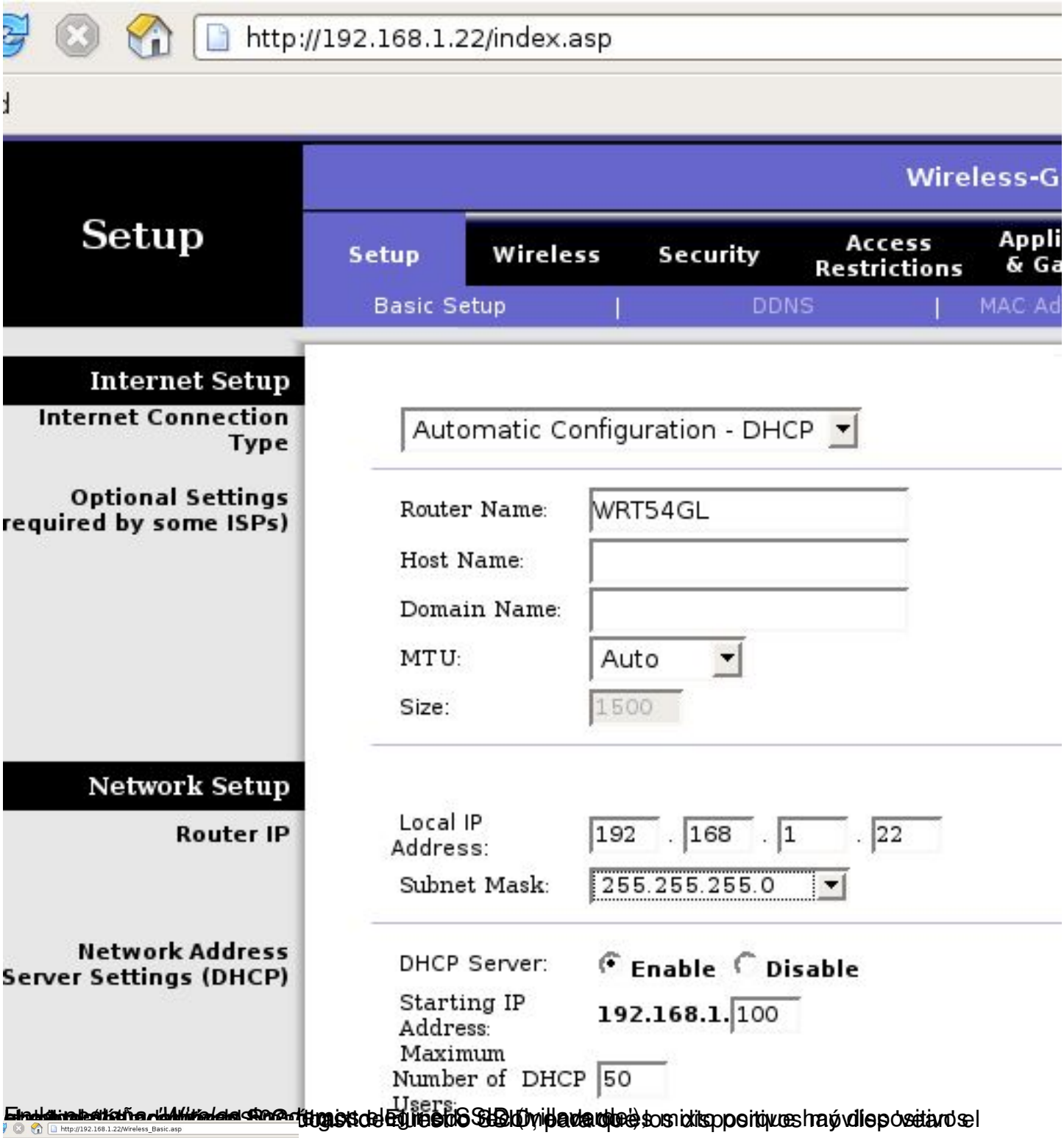
Si por casualidad se nos olvidara la IP, deberíamos resetear el router apretando un botón en la parte posterior del AP.

El router que nos da acceso a Internet nos da IP's por DHCP[6] desde la 192.168.1.2 hasta la 192.168.1.100 (para aulas y despachos que están cableados). Utilizaremos las restantes para nuestra red Wifi.

En la pestaña *'Setup'* podemos ver la asignación dinámica de la IP, *'Automatic Configuration-DHCP'* lo que significa que la IP Wifi y el DNS nos lo proporcionará el router 'principal' del centro.

También vemos que la *Local IP Adress* es *192.168.1.22,* es decir, la IP para la configuración del AP.

Por último hemos elegido que cada AP 'reparta' IP's a los dispositivos móviles que se conecten a él (*'DHCP Server: Enable'), a*sí la configuración será más fácil. Vemos que podemos limitar el número de usuarios por AP, en este caso está marcado un límite de 50.



[illegible] todos los AP's sería ésta. (Los canales repetidos no se solapan al estar

CONSIDERACIONES FINALES WIFI

En cuanto a la red Wifi el trabajo que resta es observar el funcionamiento de la red, habrá un aumento de usuarios y se incrementará el tráfico, también puede haber zonas con interferencias o por el contrario lugares sin cobertura.

Entre los aspectos a mejorar están:

- La seguridad (no hemos implementado Wep ó WPA para que la configuración sea más fácil)
- Los AP's en principio estarán colocados en aulas o despachos, se pueden instalar en los techos más adelante.
- Habrá que instalar un proxy para evitar accesos fraudulentos, maliciosos o simplemente inapropiados.

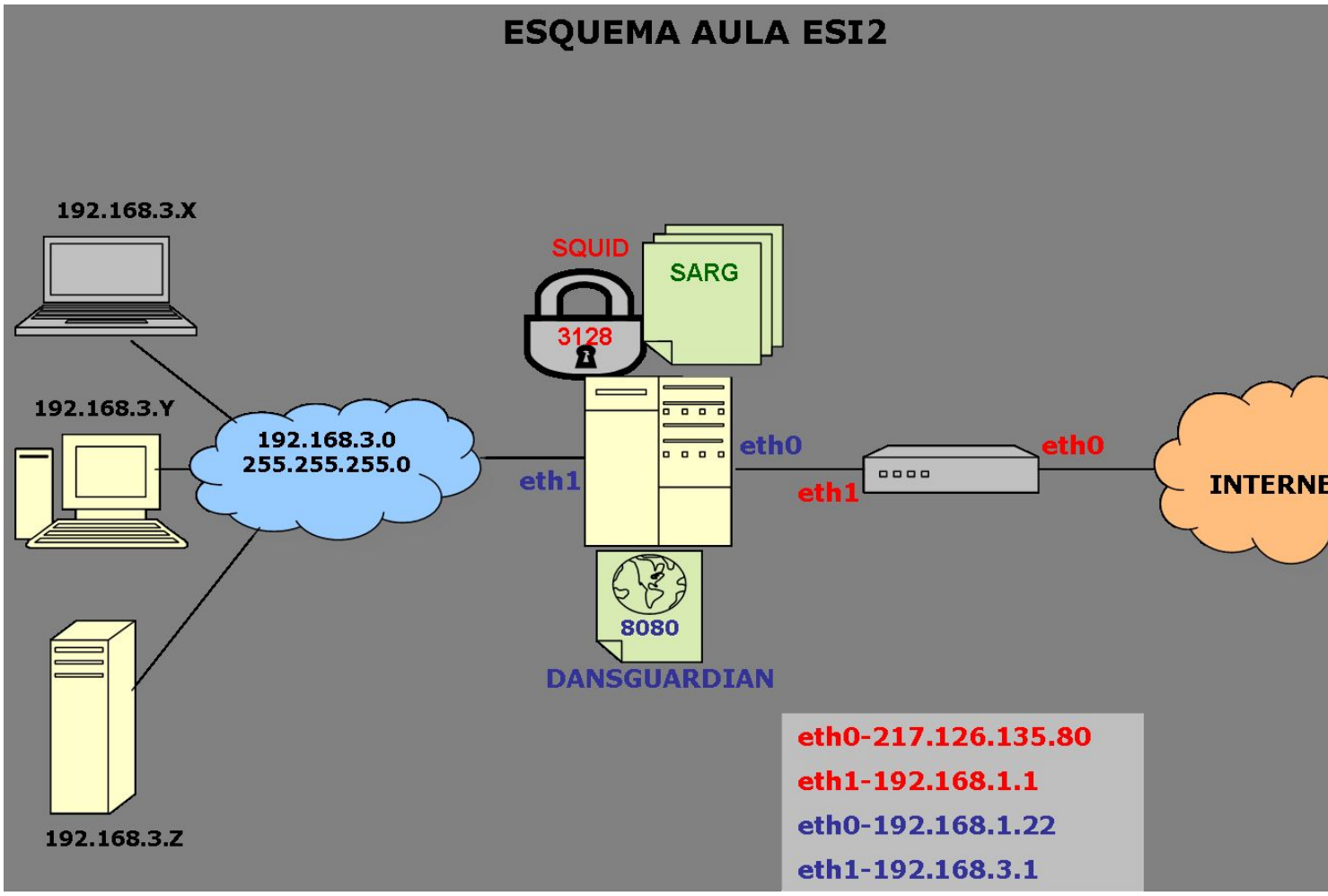
INSTALACIÓN DEL FILTRO.

Como hemos comentado antes, nuestro instituto tiene un ciclo de grado medio de informática, ESI
(Explotación de sistemas informáticos). Los alumnos de este ciclo suelen tener interés por la tecnología, pero a veces hacen un uso indebido de la conexión a Internet,utilizando el aula como un cibercafé; Es decir visitan páginas de correo, chat, redes sociales, juegos o-n-line, bajan música o archivos que no tienen nada que ver con los estudios, o simplemente acceden a páginas según sus hobbies (automóviles, deportes, moda etc.).

Una solución es privarles del acceso a Internet, pero otra más interesante es prohibir el acceso a páginas de diversas temáticas o a páginas concretas (aunque siempre irán encontrando otras), dejando la conexión para el resto de direcciones .

Para realizar este filtro, vamos a utilizar Squid[7], Dansguardian[8] y Sarg[9]. Necesitaremos instalar Apache [10] y nos
podemos ayudar de Webmin
[11]
(interfaz gráfica para administrar sistemas Unix).

Este es el esquema de un aula de informática. En las tres aulas del ciclo ESI instalaremos el filtro de forma similar.



Para configurar el filtro tenemos dos opciones, hacerlo de forma transparente o no transparente.

La primera opción es la más 'limpia' ya que el pc cliente no tiene que configurar nada. El usuario no se da cuenta de que pasa a través de un proxy hasta que éste le prohiba un acceso a una página determinada. Esta opción también es la más laboriosa ya que requiere la configuración de un firewall. Por ejemplo IPTABLES.

Ha de estar colocado entre el proxy y el router.

El proxy transparente requiere configurar el cortafuegos para que reenvíe todas las peticiones que se hagan a un puerto 80 hacia el puerto 3128 que utiliza SQUID, pero como hemos instalado DansGuardian entre ambos, es éste quien recibe la petición y la filtra.

Por lo tanto en el cortafuegos IPTABLES, debemos redirigir el tráfico saliente del puerto 80 al puerto 8080. De esta forma

#iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080

En nuestro IES nos hemos decantado por la opción 'no transparente', ya que es más flexible. En cualquier momento podemos 'saltarnos' el proxy si es necesario. Además cada aula tiene unas necesidades específicas. El único inconveniente es que hay que configurar el navegador para que salga a través del proxy. Si queremos que esta configuración esté de forma permanente podemos utilizar políticas de seguridad del sistema operativo para que el alumno no pueda acceder a la configuración de la red.

Nuestra experiencia nos dice que es mejor permitir este acceso a la configuración de la red ya que en los ciclos de informática hay módulos concretos que requieren que el alumno experimente con estas configuraciones.

Como comentamos en el primer punto de este documento hay dos redes diferenciadas; nosotros aplicaremos el filtro a las aulas de ESI, en cada una de ellas utilizaremos un servidor Proxy, que tendrá dos tarjetas de red.

La interfaz eth0 tendrá una IP de la red 192.168.1.0/24. Hay que tener en cuenta que la IP del router es 192.168.1.1/24.

La interfaz eth1 del servidor proxy tendrá una IP de la red 192.168.2.0 (ESI1),192.168.3.0

(ESI2) , ó 192.168.4.0 (ESI_TALLER).

En esta interfaz configuraremos un servidor dhcp que 'repartirá' IP'S a los equipos de cada aula.

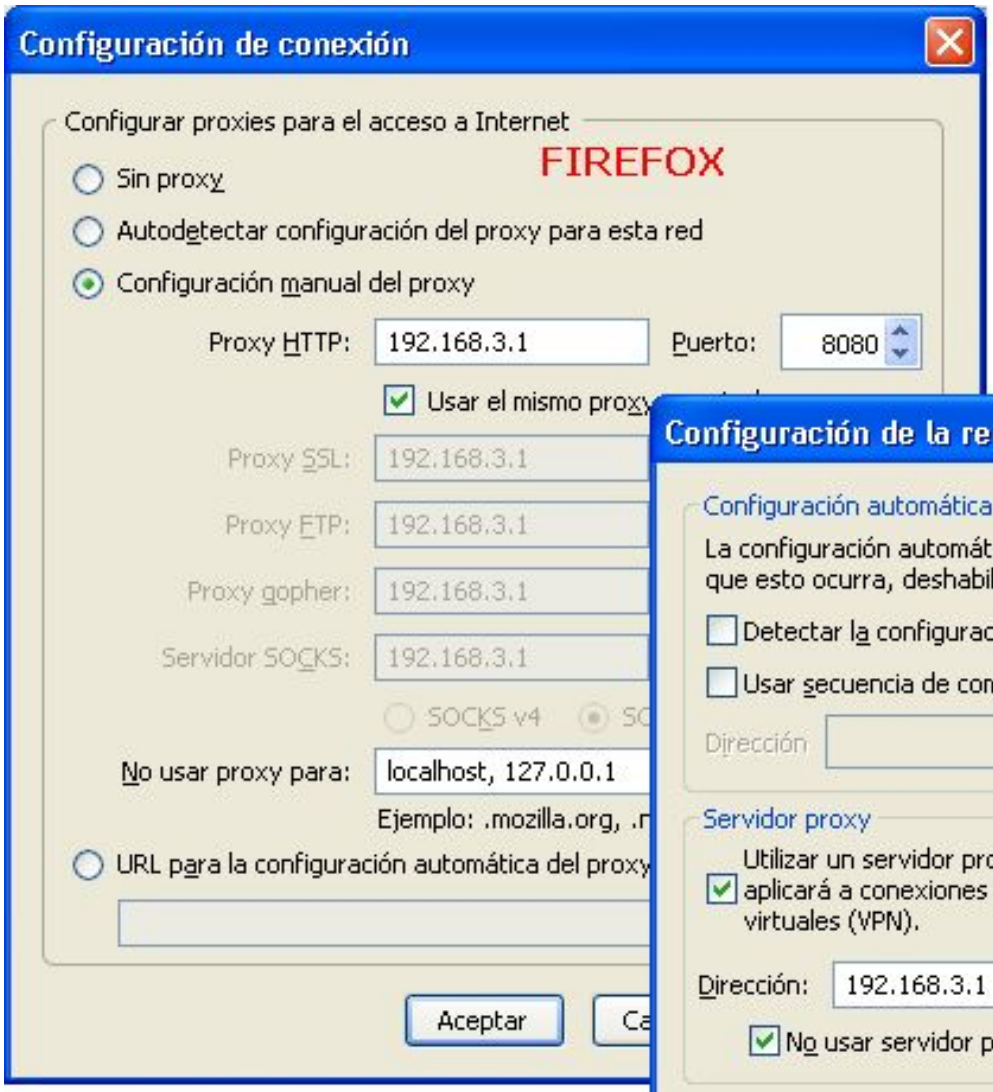
En definitiva para acceder a Internet, los equipos de cada aula habrán de configurar su navegador con la IP y puerto de su servidor proxy.

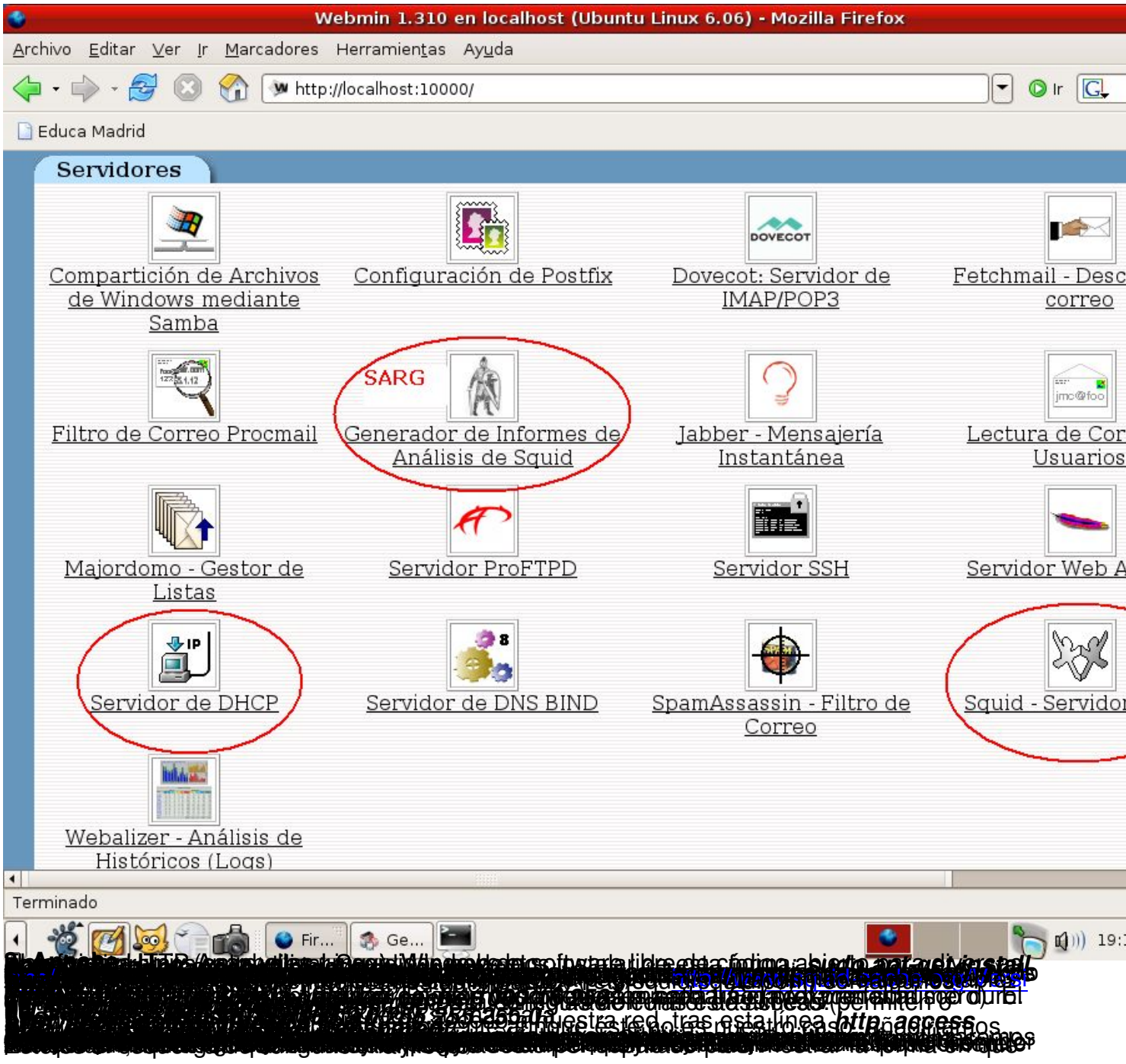
En Mozilla FireFox:

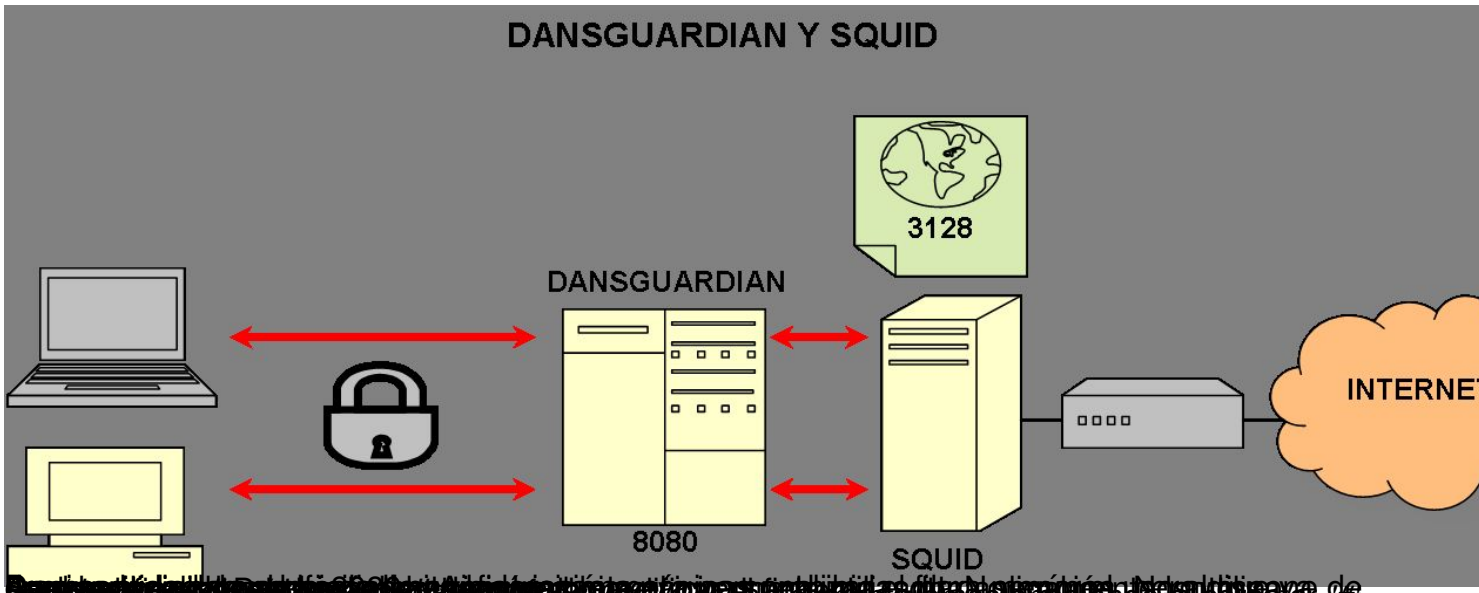
Herramientas/Opciones/Red/Configuración.

En Internet Explorer:

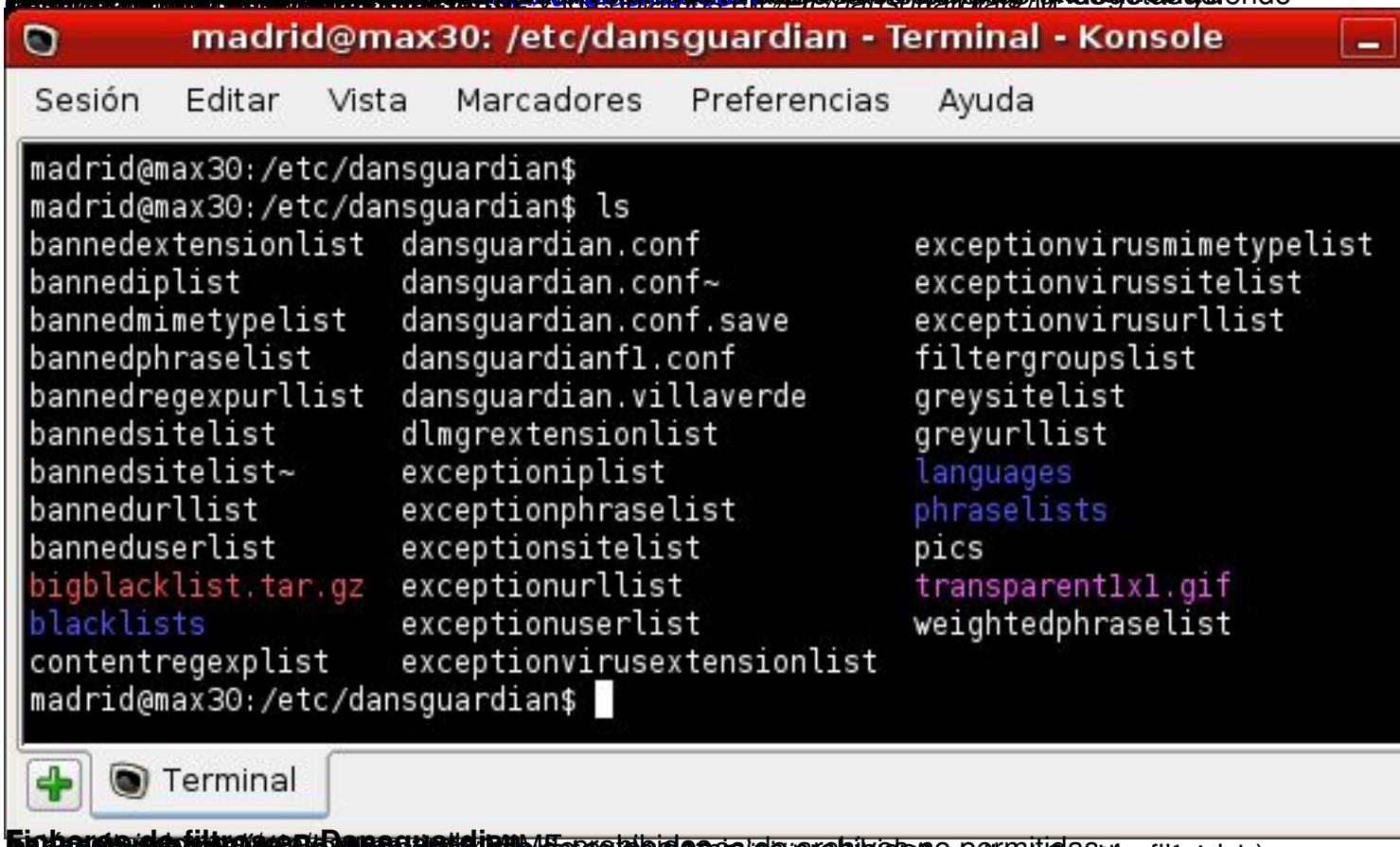
Herramientas/Opciones de Internet/Conexiones/Configuración de LAN.


Configuración de conexión
Configurar proxies para el acceso a Internet
FIREFOX
Sin proxy
Autodetectar configuración del proxy para esta red
Configuración manual del proxy
Proxy HTTP:
192.168.3.1
Puerto:
8080
Usar el mismo proxy
Proxy SSL:
192.168.3.1
Proxy FTP:
192.168.3.1
Proxy gopher:
192.168.3.1
Servidor SOCKS:
192.168.3.1
SOCKS v4
No usar proxy para:
localhost, 127.0.0.1
Ejemplo: .mozilla.org, .n
URL para la configuración automática del proxy
Aceptar
Configuración de la red de área local (LAN)
Configuración automática
La configuración automática puede superponerse a la manual. Para
que esto ocurra, deshabilite la configuración automática.
EXPLORE
Detectar la configuración automáticamente
Usar secuencia de comandos de configuración au
Dirección
Servidor proxy
Utilizar un servidor proxy para su LAN. Esta configuración no se
aplicará a conexiones de acceso telefónico o de redes privadas
virtuales (VPN).
Dirección:
192.168.3.1
Puerto:
8080
Opciones avan
No usar servidor proxy para direcciones locales
Aceptar

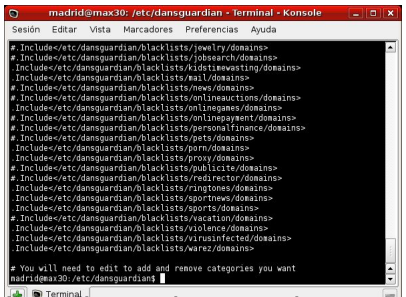

Webmin 1.310 en localhost (Ubuntu Linux 6.06) - Mozilla Firefox
Archivo Editar Ver Ir Marcadores Herramientas Ayuda
http://localhost:10000/
Ir
Educa Madrid
Servidores
Compartición de Archivos de Windows mediante Samba
Configuración de Postfix
Dovecot: Servidor de IMAP/POP3
Fetchmail - Desc correo
Filtro de Correo Procmail
SARG
Generador de Informes de Análisis de Squid
Jabber - Mensajería Instantánea
Lectura de Cor Usuarios
Majordomo - Gestor de Listas
Servidor ProFTPD
Servidor SSH
Servidor Web A
Servidor de DHCP
Servidor de DNS BIND
SpamAssassin - Filtro de Correo
Squid - Servidor
Webalizer - Análisis de Históricos (Logs)
Terminado



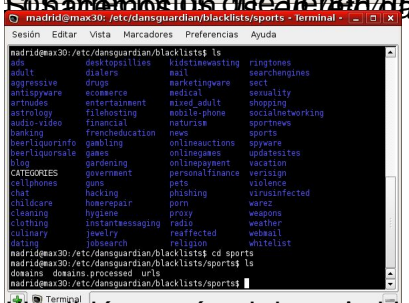
[illegible] que tengan efecto los cambios [illegible] adiendo



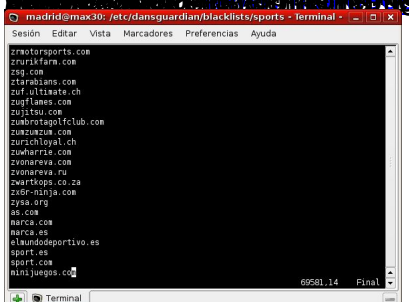
[illegible] o



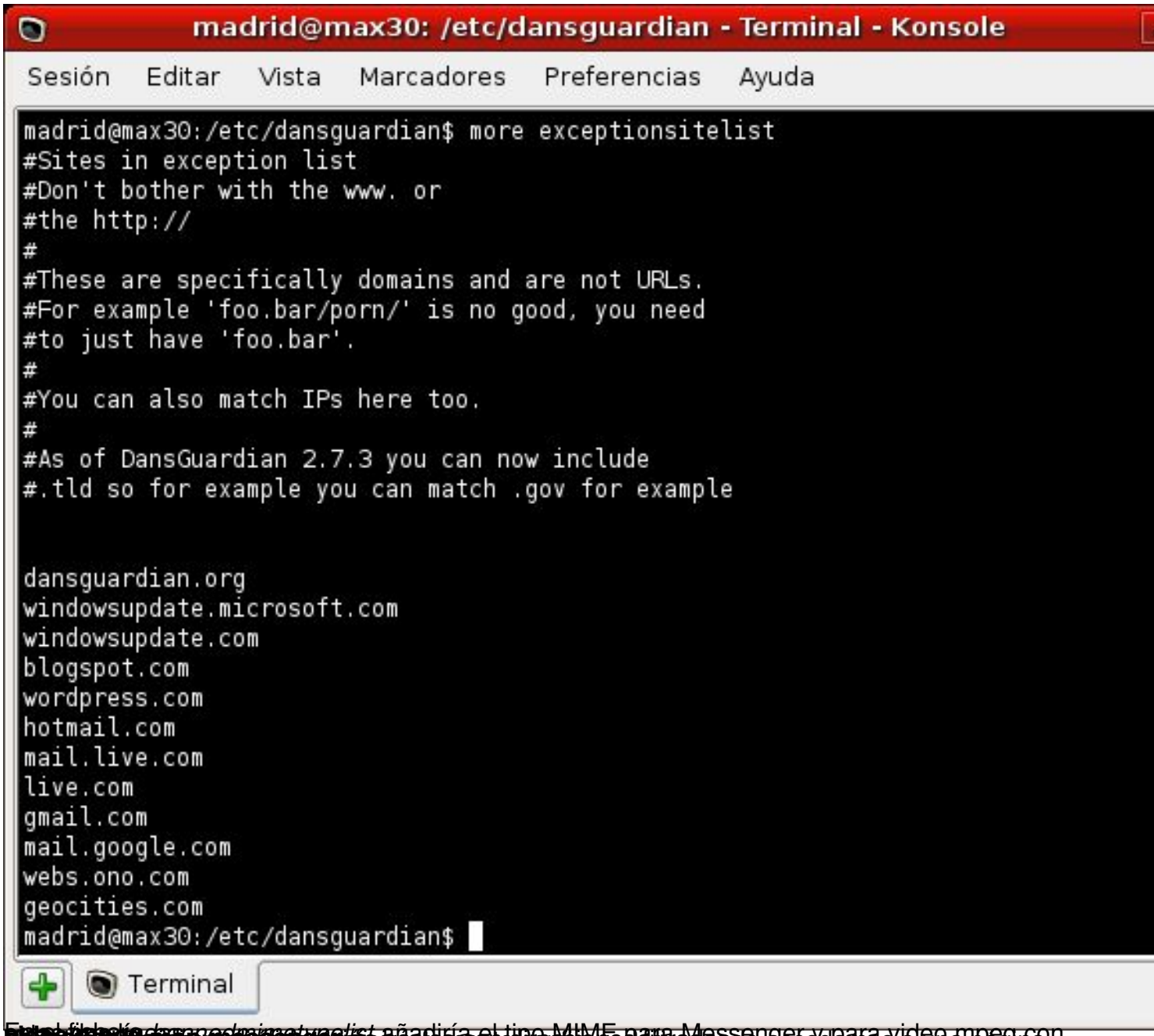
Si observamos que dentro de */etc/dansguardian/blacklists* vemos todas las listas.



Si observamos el directorio *sports* podemos ver que hay tres ficheros, uno de ellos es *domains* donde hemos añadido algunas direcciones para bloquear en el

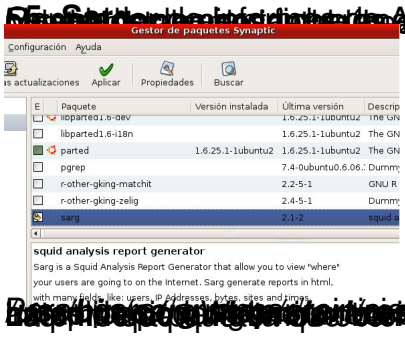


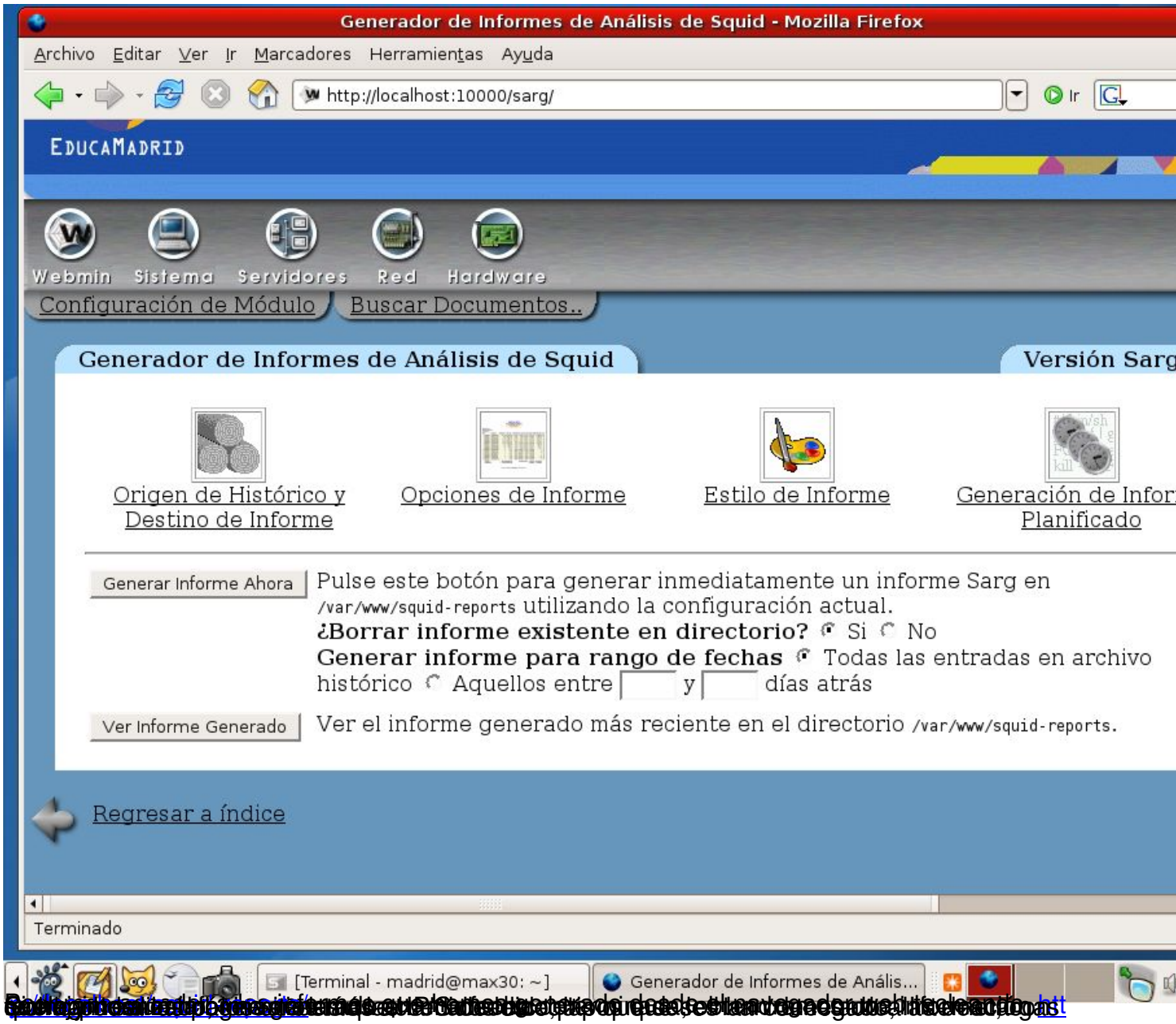
Por ejemplo, *sport.es*, *sport.com* y *minijuegos.com*. Añadiremos algunas web en las que dejaba entrar (algún blog del

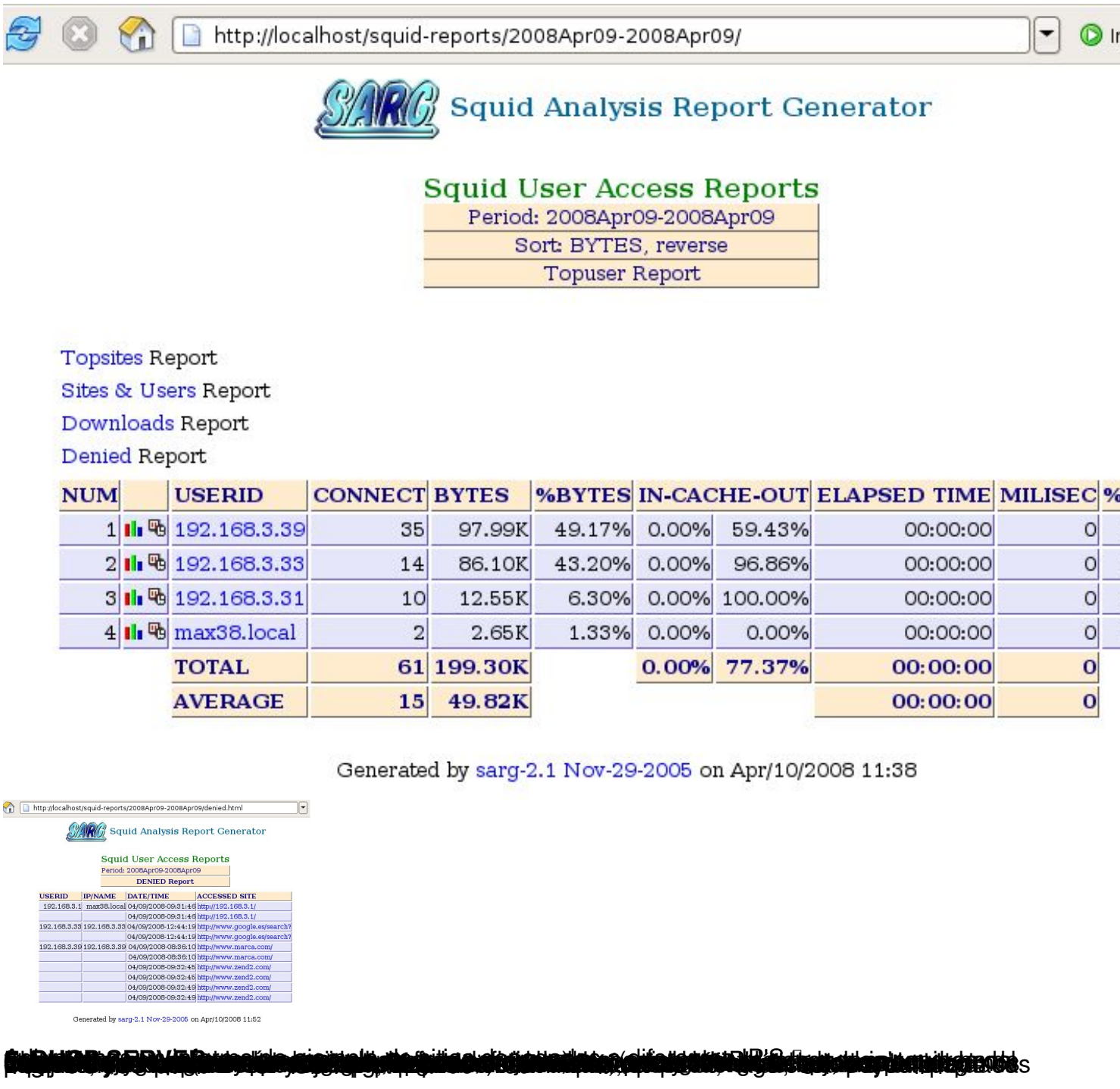


Editando el fichero */etc/dansguardian/exceptionsitelist* añadiría el tipo MIME para Messenger y para video mpeg con [illegible] estarán bien configurados, cuando accedamos a una página

http://www.marca.com/
Acceso denegado!
El acceso a la página web
http://www.marca.com
ha sido denegado por la siguiente razón:
Sitio no permitido: marca.com
Usted está viendo este mensaje de error porque la pág
que
intenta acceder contiene, o está clasificada como conte
material que se considera inapropiado.
Si tiene preguntas, por favor póngase en contact
con el Administrador de Sistemas o el Administrador de
SU COMPANIA
Powered by DansGuardian

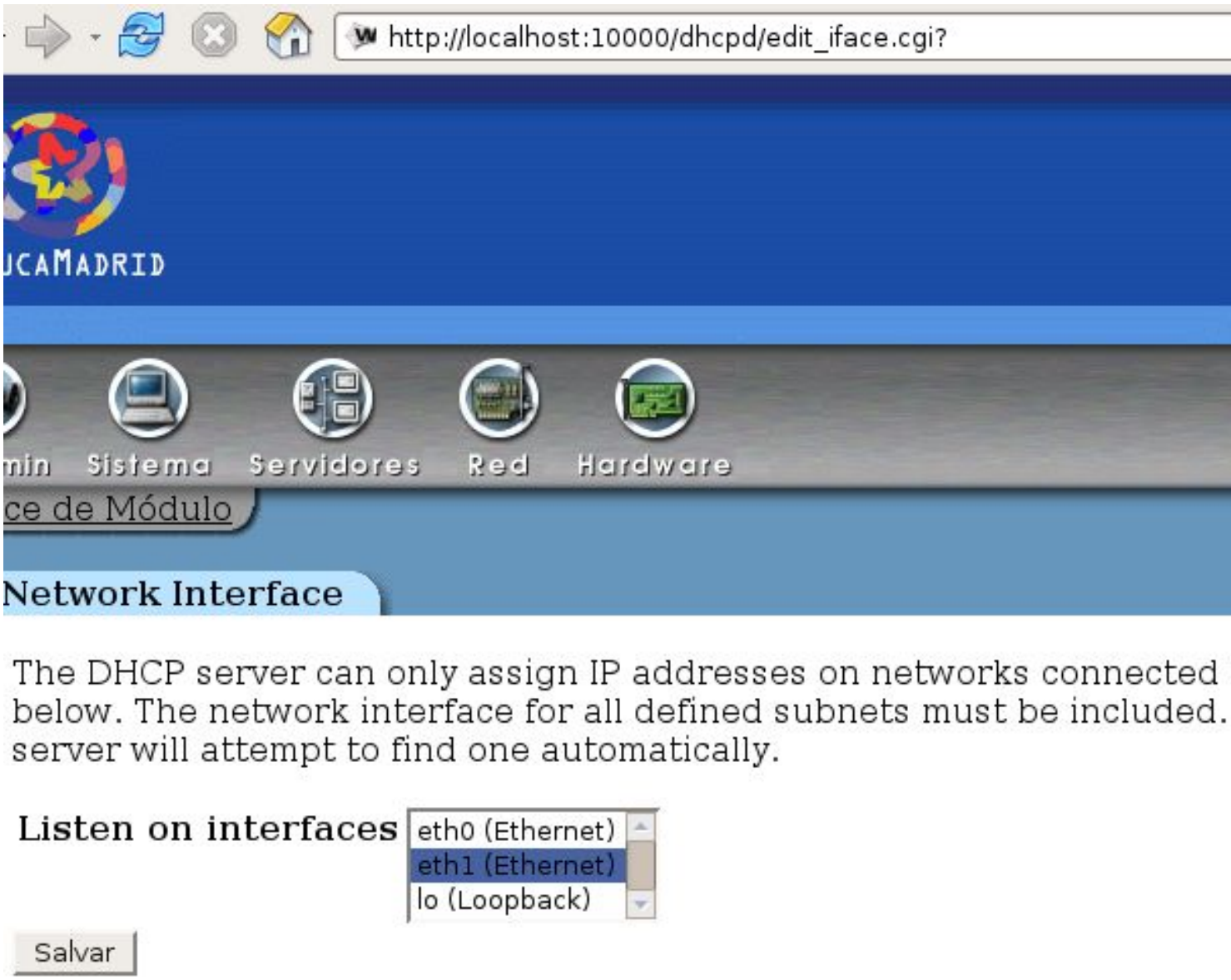

Gestor de paquetes Synaptic
Configuración Ayuda
Aplicar
Propiedades
Buscar
Paquete
Versión instalada
Última versión
parted
1.6.25.1-1ubuntu2
pgrep
r-other-gking-matchit
r-other-gking-zelig
sarg
squid analysis report generator
Sarg is a Squid Analysis Report Generator that allow you to view "where"
your users are going to on the Internet. Sarg generate reports in html,


Generador de Informes de Análisis de Squid - Mozilla Firefox
Archivo Editar Ver Ir Marcadores Herramientas Ayuda
http://localhost:10000/sarg/
Ir
EDUCAMADRID
Webmin
Sistema
Servidores
Red
Hardware
Configuración de Módulo
Buscar Documentos..
Generador de Informes de Análisis de Squid
Versión Sarg
Origen de Histórico y Destino de Informe
Opciones de Informe
Estilo de Informe
Generación de Infor Planificado
Generar Informe Ahora
Pulse este botón para generar inmediatamente un informe Sarg en /var/www/squid-reports utilizando la configuración actual.
¿Borrar informe existente en directorio? Si No
Generar informe para rango de fechas Todas las entradas en archivo histórico Aquellos entre y días atrás
Ver Informe Generado
Ver el informe generado más reciente en el directorio /var/www/squid-reports.
Regresar a índice
Terminado
[Terminal - madrid@max30: ~]
Generador de Informes de Anális...


http://localhost/squid-reports/2008Apr09-2008Apr09/
Squid Analysis Report Generator
Squid User Access Reports
Period: 2008Apr09-2008Apr09
Sort: BYTES, reverse
Topuser Report
Topsites Report
Sites & Users Report
Downloads Report
Denied Report
NUM USERID CONNECT BYTES %BYTES IN-CACHE-OUT ELAPSED TIME MILISEC
1 192.168.3.39 35 97.99K 49.17% 0.00% 59.43% 00:00:00 0
2 192.168.3.33 14 86.10K 43.20% 0.00% 96.86% 00:00:00 0
3 192.168.3.31 10 12.55K 6.30% 0.00% 100.00% 00:00:00 0
4 max38.local 2 2.65K 1.33% 0.00% 0.00% 00:00:00 0
TOTAL 61 199.30K 0.00% 77.37% 00:00:00 0
AVERAGE 15 49.82K 00:00:00 0
Generated by sarg-2.1 Nov-29-2005 on Apr/10/2008 11:38

http://localhost/squid-reports/2008Apr09-2008Apr09/denied.html
Squid Analysis Report Generator
Squid User Access Reports
Period: 2008Apr09-2008Apr09
DENIED Report
USERID IP/NAME DATE/TIME ACCESSED SITE
192.168.3.1 max38.local 04/09/2008-09:31:46 http://192.168.3.1/
04/09/2008-09:31:46 http://192.168.3.1/
192.168.3.33 192.168.3.33 04/09/2008-12:44:19 http://www.google.es/search?
04/09/2008-12:44:19 http://www.google.es/search?
192.168.3.39 192.168.3.39 04/09/2008-08:36:10 http://www.marca.com/
04/09/2008-08:36:10 http://www.marca.com/
04/09/2008-09:32:45 http://www.zend2.com/
04/09/2008-09:32:45 http://www.zend2.com/
04/09/2008-09:32:49 http://www.zend2.com/
04/09/2008-09:32:49 http://www.zend2.com/
Generated by sarg-2.1 Nov-29-2005 on Apr/10/2008 11:52

Debemos elegir el interfaz, por le que se realizará el DHCP



Ejemplo de arrendamientos DHCP, hechos por nuestro servidor:

Dirección IP	Ethernet	Nombre de máquina	Fecha de Inicio	Fecha de Fin
192.168.3.36	00:13:d4:9e:03:e5	inf02-02	2009/04/01 08:05:36	2009/04/01 08:15:36
192.168.3.47	00:c0:9f:4b:8d:b4		2009/03/25 13:40:58	2009/03/25 13:50:58
192.168.3.34	00:21:5a:16:85:1a	PC397844	2009/02/24 20:14:19	2009/02/24 20:24:19
192.168.3.41	00:13:d4:ba:b4:6b	IES-7267E0B9FFF	2009/02/24 13:42:17	2009/02/24 13:44:17
192.168.3.39	00:13:d4:ba:b4:6b	IES-7267E0B9FFF	2009/02/24 13:42:17	2009/02/24 13:44:17
192.168.3.45	00:13:d4:ba:b3:b0	EQUIP03	2009/02/24 13:34:41	2009/02/24 13:36:41

CONCLUSIONES SOBRE LA APLICACIÓN DEL FILTRO.

Por nuestra experiencia en Institutos de Educación Secundaria y Centros de Formación Profesional, consideramos que las herramientas que filtran el acceso a Internet son necesarias.

Aunque esta solución pueda parecer complicada no lo es en absoluto simplemente un poco laboriosa, y cumple perfectamente con el cometido, además de ser bastante flexible, ya que se puede modificar en cada aula.No obstante tiene algunas mejoras como la evolución hacia un filtro transparente con Iptables.

BILIOGRAFÍA Y ENLACES.

-

Comunicaciones en redes WLAN.José M. Huidobro Moya y David Roldán Martínez. Creaciones Copyright.

-

Software libre para análisis de redes 802.11.Detecta AP's *www.netstumbler.org*

-

Linksys. http://www.linksys.es/

-

Wikipedia. *http://es.wikipedia.org/wiki/Wikipedia:Portada*

-

Revista Linux. *http://www.linux-magazine.es*

-

Squid. *http://www.squid-cache.org/*

-

Squid. *http://www.deckle.co.za/squid-users-guide/Main_Page*

-

Squid. *http://www.redes-linux.com/compartir.php*

-

Dansguardian. *http://dansguardian.org/*

-

Sarg. *http://sarg.sourceforge.net/sarg.php*

-

Sarg. Página de programadores de centros educativos de Extremadura. *http://administradores.educarex.es/wiki/index.php/SARG.*

-

Para saber más sobre Squid.

http://observatorio.cnice.mec.es/modules.php?op=modload&name=News&file=article&sid=589 .

-

Profundizar en Apache. http://observatorio.cnice.mec.es/modules.php?op=modload&name=News&file=article&sid=580

-

Más sobre Dansguardian.
http://observatorio.cnice.mec.es/modules.php?op=modload&name=News&file=article&sid=524

NOTAS

[1] ICM. Informática de la Comunidad de Madrid

[2] Nivel de enlace. Nivel 2 en el modelo OSI (Interconexión de Sistemas Abiertos).

[3] WEP. Wireless Equivalent Privacy. Esquema de encriptación que protege los datos intercambiados entre los dispositivos móviles y los puntos de acceso.

[4] WPA. Wifi Protected Access. Mejora el WEP. Claves de más de 128 bits.

[5] RADIUS. (Remote Authentication Dial In User Server). Validación por usuario/password frente a estos servidores. Normalmente se utilizan túneles VPN.

[6] DHCP (Dynamic Host Configuration Protocol). Protocolo de red que permite a los nodos de una red obtener sus parámetros de configuración automáticamente como la IP, DNS etc..

[7]Squid. Programa de software libre que implementa un servidor proxy y caché web. Licencia

GPL.

[8] DansGuardian. Es un filtro de contenidos de sitios web.Se sitúa entre el navegador cliente y el proxy, interceptando y modificando la comunicación entre ambos. *http://dansguardian.org*

[9] Sarg. Analizador de ficheros de registro del Squid. *http://sarg.sourceforge.net/sarg.php*

[10] Apache. Servidor web HTTP de código abierto. *http://httpd.apache.org/*

[11] Webmin. Intterfaz gráfica para administrar sistemas Unix. *http://www.webmin.com*