Herramientas *Open Source*

Autor: Sergi Tur Badenas

Que es *Open Source*?

Que es *Open Source*?

Autor: Sergi Tur Badenas

DAFO

Duplicación de esfuerzos

Falta de productos en determinados segmentos

DEBILIDADES

Desconocimiento

Costos de cambio altos

Derechos de autor

Patentes de software

Falta de profesionales cualificados

AMENAZAS

FORTALEZAS

Diversificación de intereses
Estándares abiertos
Multiplataforma
Multilingüismo
Personalización
Independencia del proveedor
Coste
Importancia generalizada

OPORTUNIDADES

Crecimiento en un entorno de libre competencia

Bajo coste de oportunidad

http://www.culturalliure.cat/llibre/programari-lliure-i-empresa-a-catalunya/analisi-dafo/

Autor: Sergi Tur Badenas

Debilidades

- **Duplicación de esfuerzos**
  - Aunque todo el mundo reconoce que la diversidad de opciones es buena y que la tendencia es, que incluso las empresas competidoras colaboren en un mismo proyecto, algunos proyectos con objetivos idénticos podrían avanzar si unificaran esfuerzos.
  - Sin ir más lejos la multitud de distribuciones GNU/Linux
- **Falta de productos en determinados segmentos**
  - Todavía hay segmentos de mercado en los que el software libre, no puede ofrecer ningún producto.

Autor: Sergi Tur Badenas

Amenazas

- **Desconocimiento**
  - El software libre parte de un alto grado de desconocimiento por parte de los usuarios, profesionales del sector y responsables TIC. Todavía es habitual **confundir** SL con **software gratuito** o que se cuestione la existencia de servicios profesionales dirigidos a la empresa.
- **Costos de cambio altos**
  - Los formatos privativos, la migración de datos, los contratos de licencia existentes, la curva de aprendizaje de los usuarios y de los responsables son algunos de los retos a los que se enfronta una empresa que quiere migrar a soluciones libres. Muchos de estos costes son comunes a otro tipo de migraciones
  - A menudo es más fácil comenzar con soluciones libres en proyectos nuevos que en proyectos existentes.

Autor: Sergi Tur Badenas

Amenazas

- **Derechos de autor**
  - En 2003 SCO comenzó a demandar empresas usuarias de GNU/Linux, entre les cuales IBM, por una supuesta violación de derechos de autor.
  - Las licencias permiten a los desarrolladores, usuarios y proyectos disponer de protección jurídica frente a posibles reclamaciones legales.
- **Patentes de software**
  - Las patentes en el mundo del software permiten que las empresas con mas recursos económicos y legales establezcan barreras de acceso a las nueva tecnologías impidiendo la innovación de otras empresas, aumentando innecesariamente los costos de desarrollo de software.

Autor: Sergi Tur Badenas

Amenazas

- **FUD (Fear Uncertainty & Doubt)**: Crean una incertidumbre en las empresas desarrolladores de software ya que en cualquier momento pueden infringir una patente sin saberlo. Representan una amenaza muy importante para la industria del software en general y para el SL.

- **Falta de profesionales cualificados**
  - Todo y que se han ido consolidando empresas proveedoras TIC con capacidad y experiencia para trabajar con SL, aún cuesta encontrar personal cualificado.
  - La presencia del SL ha ido aumentando en las universidades, en programas de formación continuada y en estudios reglados.
  - Todavía hay un grupo importante de profesionales de la informática que desconocen la tecnología y que tienen un poder decisivo en la evaluación y la toma de decisiones.

Autor: Sergi Tur Badenas

Fortalezas

- **Diversificación de intereses**
  - En muchos proyectos SL convergen intereses de voluntarios, empresas, universidades, etc. generando sinergias muy interesantes.
- **Estándares abiertos.**
  - El SL ofrece un soporte excelente y soporta perfectamente los estándares abiertos (p.ej. tecnologías web y de red). OpenDocument --> OpenOffice.org.
- **Multiplataforma.**
  - Muchas de las aplicaciones libres están disponibles en MAC, Windows y Linux.

Autor: Sergi Tur Badenas

Fortalezas

- **Plurilingüismo**
  - En el mundo privativo, las traducciones solo las puede hacer el fabricante del software. Con el acceso al código fuente cualquiera puede traducir una aplicación.
- **Adaptación**
  - El software privativo se vende en forma de paquete estándar que a menudo no se adapta a las necesidades de una empresa o profesional.
  - Al disponer del código fuente es mas fácil adaptar el software. La personalización es una área muy importante en la que el SL puede responder mucho mejor que el privativo y a costes mas razonables
  - Gran parte de la industria del software se basa (y debería basar-se más) en la adaptación y en los servicios añadidos.

Autor: Sergi Tur Badenas

Fortalezas

- **Independencia del proveedor.**
  - Uno de los grandes problemas de la industria del software es la dependencia que se crea entre fabricante y cliente.
  - Si el fabricante no libra el el código fuente del producto el cliente que inevitablemente ligado a nuevas versiones y a cualquier mejora que necesite.
  - La disponibilidad del código fuente garantiza una independencia respecto al proveedor. Cualquier empresa o profesional con los conocimientos adecuados, puede continuar ofreciendo los servicios o el desarrollo de la aplicación

Autor: Sergi Tur Badenas

Fortalezas

- **Coste**
  - Factor importante, y a veces determinante en la elección de nuevos sistemas informáticos
  - El software libre no solo no tiene coste de licencia sino que además los costes de administración a menudo son inferiores a los de plataformas privativas
- **Importancia generalizada**
  - Organizaciones con fuertes recursos como IBM, Google, la NASA o SUN y muchos gobiernos de todo el mundo, utilizan SL como parte de su infraestructura y colaboran en las mejoras y el desarrollo.
  - El SL es cada vez mas importante para empresas y personas

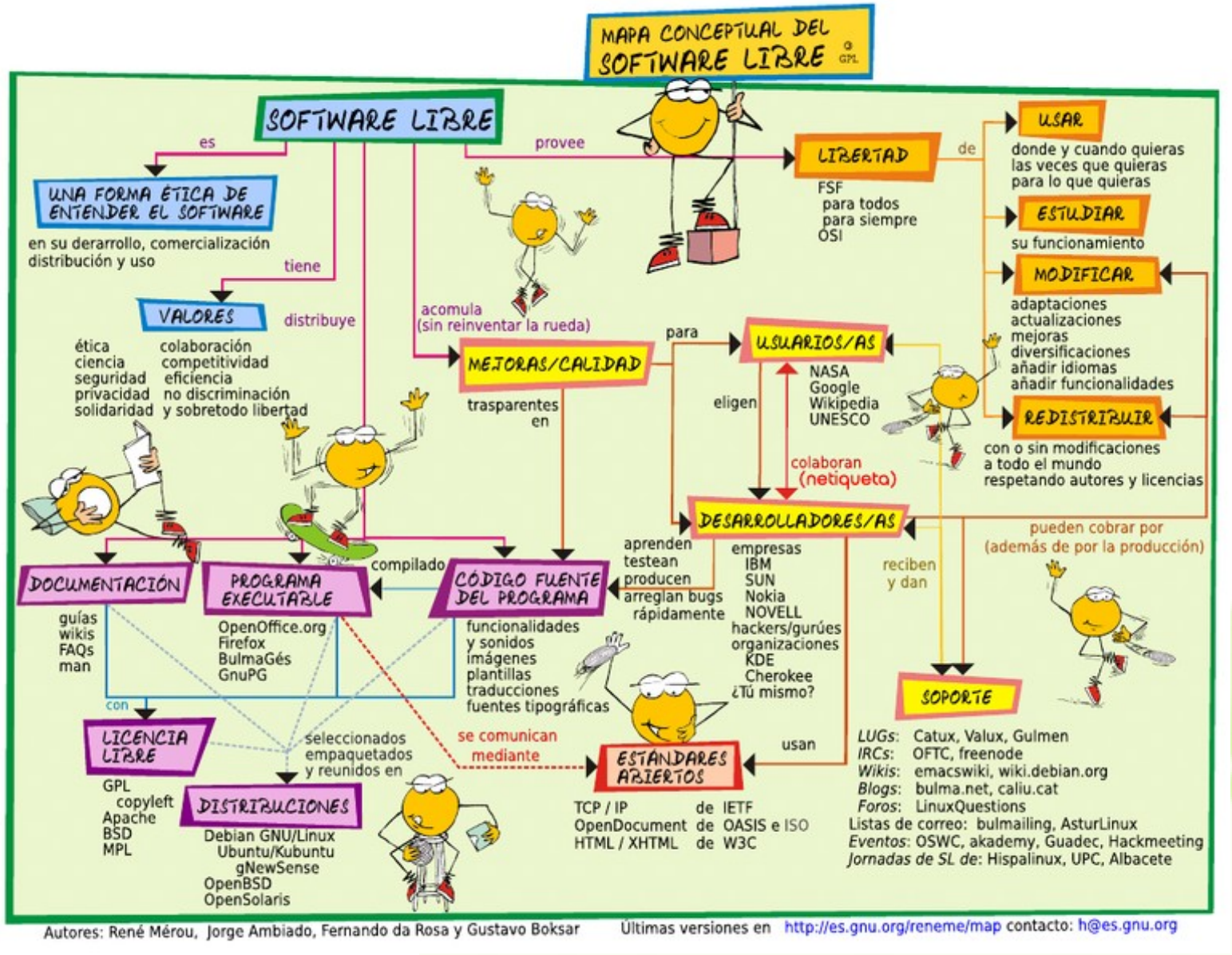
Autor: Sergi Tur Badenas

Oportunidades

- **Crecimiento en un entorno libre de competencia**
  - El SL esta experimentando un fuerte crecimiento y el número de productos y servicios es cada vez mas grande. La filosofía del SL, según la cual nadie tiene el monopolio de desarrollo ni distribución, tiene como consecuencia un entorno competitivo beneficioso para los usuarios, emprendedores y PyMEs.
- **Bajo coste de oportunidad.**
  - Hay miles de aplicaciones de SL que podemos utilizar para construir soluciones nuevas con un coste bajo de oportunidad. Además, la distribución de software a través de Internet y los sistemas de paquetes de distribuciones GNU/Linux ponen a nuestra disposición un gran numero de usuarios de forma gratuita

Autor: Sergi Tur Badenas

Software libre



Autor: Sergi Tur Badenas

Las 4 libertades


Richard Stallman

- **Libertad 0: Libertad de usar**
  - La libertad de usar el programa, con cualquier propósito
- **Libertad 1: Libertad de estudiar**
  - La libertad de estudiar cómo funciona el programa, y adaptarlo a tus necesidades.
- **Libertad 2: Libertad de distribuir**
  - La libertad de distribuir copias. Software legal.
- **Libertad 3: Libertad de modificar**
  - La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie.

Autor: Sergi Tur Badenas

Licencias

El software libre **no es software de dominio público**. Requiere de licencia

- **Diferentes tipos de licencias libres**
  - **"No víricas"**
    - Se puede crear una obra derivada sin que ésta tenga obligación de protección alguna.
    - Apache Software License v.1.1, **BSD License**, MIT License...
  - **Víricas**
    - Algunas restricciones se aplican a las obras derivadas.
    - GNU General Public License v.2.0.
    - GNU General Public License v.3.0.
    - GNU Lesser General Public License v.2.1.
    - Mozilla Public License

Autor: Sergi Tur Badenas

Copyleft

Copyleft o copia permitida (=left(de leave)) =granted comprende a un grupo de derechos de autor caracterizados por **eliminar las restricciones de distribución o modificación** impuestas por el copyright, con la **condición** de que el trabajo derivado se mantenga con el **mismo régimen de derechos de autor que el original.**

- **Creative Commons**
  - La libertad aplicada a cualquier ámbito creativo
    - Programas informáticos, arte, cultura, ciencia...
  - Estas transparencias tienen copyleft

  Creative Commons

Autor: Sergi Tur Badenas

Herramientas Open Source

- **Clasificación**
  - **Servicios de infraestructura de red**
    - Comandos y utilidades de red
    - Infraestructura LAN
    - Routing. Firmwares y distribuciones Linux para redes
    - Configuración de la red : DNS y DHCP
  - **Seguridad y monitorización**
    - Seguridad en el nivel de red y transporte: Firewall iptables
    - Analizadores de red (Wireshark, tcpdump, kismet)
    - Seguridad en el nivel de aplicación. Proxy (Squid)
    - Monitorización de la red
    - Hacking Tools. Seguridad LAN
    - Intrusion Detection Systems (IDS) Snort

Autor: Sergi Tur Badenas

Herramientas Open Source

- **Servicios de red**
  - Servidor web (Apache)
    - Servidores de aplicaciones
  - Servidores de correo electrónico
  - Servidores de bases de datos (MySQL, PostreSQL, Firebird)
  - Compartición de ficheros: NFS y Samba
  - Virtual Private Networks (openVPN)
  - Voz IP (Asterisk)
- **Herramientas Open Source**
  - Acceso remoto: SSH, VPN, RDP, FreeNX
  - Terminales tontos: LTSP, DRBL
  - Virtualización: Xen, VirtualBox
  - Alta disponibilidad

Autor: Sergi Tur Badenas

Servicios de infraestructura de red

Autor: Sergi Tur Badenas

Comandos y utilidades de red

- **Los sistemas operativos Linux son una base perfecta para la gestión de redes**
  - Amplio surtido de utilidades i comandos de red

Ping, ifconfig, route, ip, traceroute, nmap, whois, netcat, arp, mii-tool, ethtool, netstat, whois, iwconfig, ipcalc, dnstracer, dig...

  - Filosofía Unix --> Pequeñas herramientas que hacen muy bien su faena
    - Operaciones complejas --> Combinación de herramientas
  - Los sistemas **Unix-like** se diseñaron desde un principio para trabajar en red.
- **Ejemplo:**
  - Solo en el repositorio de paquetes de Ubuntu/Debian existen **1383** paquetes relacionados con redes

Autor: Sergi Tur Badenas

Infraestructura de red LAN

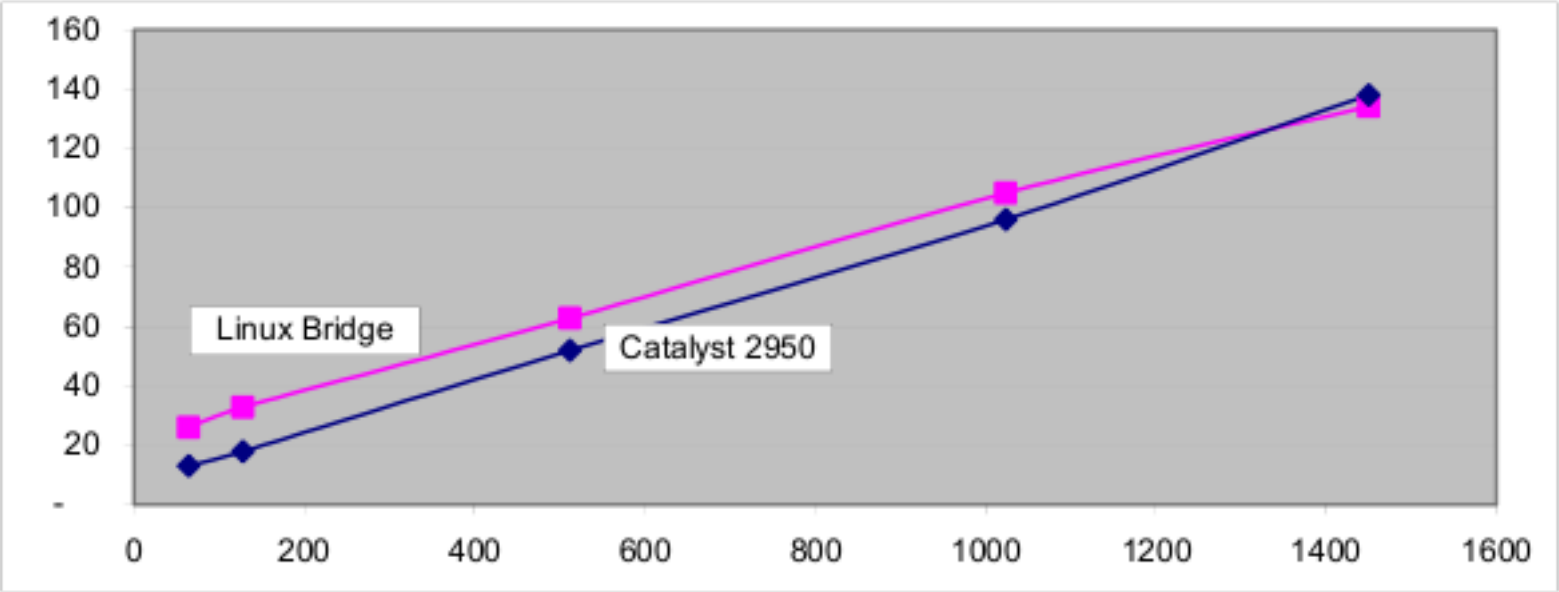
- **Puentes (bridge) entre segmentos de red**
  - Paquete bridge-utils comando **brctl**
  - Soporta Spanning-Tree Protocol (**STP**)
  - Se puede montar un conmutador en una máquina con Linux. No es habitual.
- **VLAN (Virtual LAN)**
  - Paquete y comando vlan
  - También esta soportado soportado en firmwares Linux como DD-WRT

Muchos de los comandos Unix son lo que nos encontramos en el firmware de dispositivos de red comerciales

Autor: Sergi Tur Badenas

Infraestructura de red LAN

- **Ventajas**
  - Hay estudios que equiparan la velocidad de un conmutador Linux con conmutadores comerciales.
  - Los conmutadores comerciales gestionados son caros.
  - Flexibilidad. No es necesario aprender lenguajes específicos (Cisco IOS)



Autor: Sergi Tur Badenas

Otros protocolos OSI nivel 2

- **VRRP (Virtual Router Redundancy Protocol)**
  - vrrpd: Demonio VRRP
  - KeepAlived: Sistema de redundancia y balance de carga en un pool de máquinas **LVS (Linux Virtual Server). Clustering.** Implementa también VRRPD
  - **Ucarp**: otra herramienta de failover
- **PPP (Point To Point Protocol)**
  - Paquete PPP (PPP Daemon)
- **ATM**
  - Paquete **atm-tools**
- **Multiprotocol Label Switching**
  - http://mpls-linux.sourceforge.net/

Autor: Sergi Tur Badenas

Routing

- **Static Routing**
  - Soportado por el kernel. Comandos de red (route, ip route, etc.)
- **Dinamic routing**
  - Hay soporte tanto para protocolos de routing exterior (EGP, BGP, CSPF) como interior (IGRP, EIGRP, OSPF, RIP, IS-IS). Implementaciones:
    - **GNU Zebra:** routing suite (soporta OSPF)
    - **Quagga:** fork de zebra (soporta OSPF, BGP, IS-IS y RIP)
    - **OpenBGPD:** soporta OSPF
    - **Otros:** 6WINDGate, Vyatta, XORP, BIRD, GateD
- **Firmwares Linux**
  - DD-WRT incorpora soporte para RIP, BGP y OSLR

Autor: Sergi Tur Badenas

Firmwares Linux

- **Firmwares Linux para dispositivos encastados de red**
  - Orientados al segmento SoHo (routers ADSL)
  - Superiores en opciones de control y a menudo en estabilidad
    - Muchos firmwares “comerciales” están basados en Linux

Funcionalidades

Data logging, Booting, cron, NVRAM, file editing, Linux package management, SNMP, backup and restore, Firmware upgrade, WAN, VLAN, Wi-Fi, WEP, WPA, WDS, MAC filtering, Firewall, Port forwarding, DHCP, Dnsmasq, Hostnames, IP control, Routing, UPNP, QoS, DynDNS, WoL, OpenVPN, PPTP, Hotspots.

  - Interfaz gráfica web
  - openwrt, dd-wrt, Tomato, voyage (Debian)

Autor: Sergi Tur Badenas

Distribuciones Firewall Linux

- **Distribuciones Linux para crear dispositivos de red**
  - Se usan sobretodo como routers perimetrales (firewall) de control de acceso a la red.
  - Interfaz gráfica web
  - IPCOP, m0n0wall, PFSense (BSD)

Funcionalidades

Firewall, Proxy, Filtros URL, cache de actualizaciones de software, Filtros de capa 7, bloqueo de tráfico, Monitorización, VPN, gráficas de estado de máquina y red, informes del proxy, Balanceo de carga, QoS, IDS, etc.

Autor: Sergi Tur Badenas

Firmwares Linux

- **Ventajas**
  - Aumento de funcionalidad sin aumentar el precio
  - Soporte de la comunidad. Comunidades muy activas
  - Ahorro respecto al precio de hardware equivalente con las mismas funcionalidades
  - Facilidad de adaptación
  - Mayor control (acceso remoto a una terminal Linux)
  - Se pueden ampliar las funcionalidades instalando software libre adicional.
  - A menudo ya lo estamos utilizando sin saberlo...

La FSF, hace poco (2008) ha denunciado a Cisco solicitándole cumplir los términos de la GPL en los productos de su filial Linksys, que utilizan herramientas (GCC, binutils, librería de C de GNU...) con esta licencia

Autor: Sergi Tur Badenas

Hardware para firmwares Linux

- **Cualquier PC**
  - No es necesario que sean muy potentes--> Aprovechar hardware obsoleto
- **Hardware especifico**
  - Se pueden crear dispositivos de red a partir de placas madre como **Alix**, **WRAP**, **microtik**, **Ubiquity** o placas madre mini-ITX.
  - En Catalunya tenemos la red WIFI libre más grande del mundo: guifi.net montada con “trastos” de este tipo.

Autor: Sergi Tur Badenas

Servidor DNS. Bind

- **BIND (Berkeley Internet Name Domain)**
  - Servidor DNS más utilizado --> "**Estándar de facto**"
  - Creado en la Universidad de Berkeley principios 80s
  - Gestionado por la **ISC** (Internet Systems Consortium). Paul Vixie.
  - Críticas de seguridad en las versiones iniciales. La versión actual: **bind release 9**. Reescrita desde cero.
  - Disponible en los repositorios de todas las distros Linux
  - Dispone de interfaz gráfica web utilizando **Webmin**
  - Apto tanto para grandes servidores DNS como para servidores DNS de redes locales pequeñas

Autor: Sergi Tur Badenas

Bind. Servidor DNS

- **Cuota de mercado (Octubre 2007)**

BIND 9	249,484	64.53%
Nominum CNS/Embedded Linux*	74,559	19.29%
PowerDNS	25,469	6.59%
BIND 8	21,772	5.63%
Microsoft Windows DNS 2000	6,967	1.80%
Microsoft Windows DNS 2003	3,232	0.84%
BIND 4	856	0.22%
Cisco CNR	604	0.16%
Microsoft Windows DNS NT4	394	0.10%
Other	3,251	0.84%

- **Root Name servers (10 de 13)**
  - http://en.wikipedia.org/wiki/Root_nameserver
    - **NSD** también es Open Source (BSD License)

Autor: Sergi Tur Badenas

Servidor DHCP del ISC

- **ISC (Internet Systems Consortium) DHCP**
  - Servidor de DHCP Open Source más utilizado
  - Creado en diciembre de 1997
  - Mantenido por el ISC desde 2004
  - Muchos dispositivos de hardware, como *routers* SoHo, incluyen un servidor de DHCP *Open Source* adaptado.
- **Ventajas**
  - Dispone de *failover* (múltiples DHCP Servers)
  - Fácil de configurar. Interfaz web con Webmin
  - Tanto Bind como el servidor de DHCP pueden trabajar perfectamente en **redes heterogéneas**

Autor: Sergi Tur Badenas

Seguridad y monitorización

Autor: Sergi Tur Badenas

Firewall. Iptables

Firewall Command	Linux Kernel Version
iptables	2.4.x, 2.6.x
ipchains	2.2.x
ipfwadm	2.0.x

- **Firewall de facto en Linux**
  - Máxima seguridad --> Integrado en el kernel del SO
  - Funcionalidad
    - **Filtrado de paquetes**
    - **NAT y connection tracking**
    - **Registro (log)**
    - **Gestión de colas de paquetes**
  - **Fwbuilder:** herramienta gráfica de gestión de *firewalls*
  - **Incluido** en muchos *firmwares* de routers comerciales

Autor: Sergi Tur Badenas

Analizadores de red

- **También conocidos como "packet Sniffers"**
  - Permiten registrar todo el tráfico de red en tiempo real o en ficheros de captura
  - **Wireshark** (aka **Ethereal**)
    - Estándar "de facto". Herramienta gráfica basada en tcpdump
  - **Tcpdump**: navaja suiza de los *packet sniffers*

> **Filosofía Unix**-->Cada programa debe hacer un solo trabajo y hacerlo bien, esta filosofía y la habilidad de interconectar programas lo hacen un sistema operativo modular y robusto

  - **Multiplataforma**: Se basan en una librería *Open Source* llamada **libpcap** de la cual hay un *port* a Windows (**winpcap**)

Autor: Sergi Tur Badenas

Seguridad a nivel de aplicación

- **Antivirus**

  Hay muy pocos Virus en Linux, debido a la dificultad que tienen en expandir-se (uso de usuarios si permisos de administración) y a las rápidas actualizaciones frente a vulnerabilidades.

  - **Clamav**: Muy utilizado como filtro antivirus en servidores de correo (*server-side email virus scanner*).
  - Existe una versión para Windows **clamWin**

- **Anti-SPAM**

  - **Spamassasin** es la herramienta *Open Source* mas utilizada
  - Gestionada por la Apache Software Foundation (ASF)

Autor: Sergi Tur Badenas

Seguridad a nivel de aplicación

- **Filtros P2P y otras aplicaciones**
  - **L7-filter:** parche del kernel que permite filtrar protocolos a nivel de aplicación
  - **ipp2p:** parche de iptables que permite filtrar protocolos P2P
  - Se basan en la identificación de patrones. Son bastante costosos en tiempo de ejecución.
  - A menudo están incluidas (o se pueden incluir como módulos o *plugins*) en firmwares y distros Linux para redes
  - Pueden filtrar otras aplicaciones: mensajería instantánea o chat, vídeo streaming, juegos online...

Autor: Sergi Tur Badenas

Proxy (Squid)

- **Squid (calamar en angles)**
  - El servidor *proxy* y cache web *Open Source* mas utilizado. Licencia GNU General Public License.
  - Soporta diferentes protocolos pero se utiliza principalmente para HTTP y FTP. Tiene soporte parcial para SSL y TLS.
  - Permite mejorar el rendimiento de red (cache de páginas web)
- **Squid+plugins (addons)**
  - Permite filtrar contenidos
  - SquidGuard, Calamaris, ufdbGuard...

Autor: Sergi Tur Badenas

Gestión del tráfico de una red. Monitorización

- **Infinidad de herramientas para monitorizar y realizar informes de tráfico de red**
  - iptraf,tcptrack,bwm,cutter,slurm,vnstat...
    - **Iptraf**: Muestra en tiempo real el tráfico de las conexiones
- **Monitorización**
  - La primera línea de defensa es saber que ocurre en la red
  - **Casi todas las herramientas són web --> Multiplataforma**
    - **NTOP:** Network top. “Equivalente” de la comanda top pero para la monitorización de redes.
    - **Bandwithd:** Permite monitorizar el ancho de banda utilizado en una red mediante gráficas RDD.

Autor: Sergi Tur Badenas

Monitorización

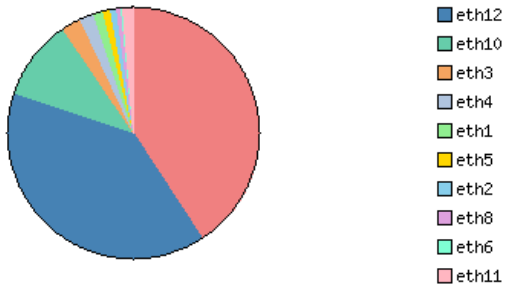
- **Simple Network Management Protocol (SNMP)**
  - Existen múltiples aplicaciones que soportan SNMP y que nos permiten gestionar la red. Podemos trabajar directamente con el protocolo y programar-lo con las bibliotecas de soporte.
- **Herramientas**
  - MRTG y RDDTOOL: Permiten crear gráficas Round Robin.
    - **Munin:** Monitoriza los recursos de servidores de la red
    - **Cacti:** Permite monitorizar dispositivos de red con soporte SNMP
  - **Nagios:** Uno de los más completos y configurables. Dispone de un sistema de alertas por e-mail, SMS..., informes de disponibilidad, trends, histogramas de alertas...
  - Y la lista continua... **monit, hobbit, zennos**...

Autor: Sergi Tur Badenas

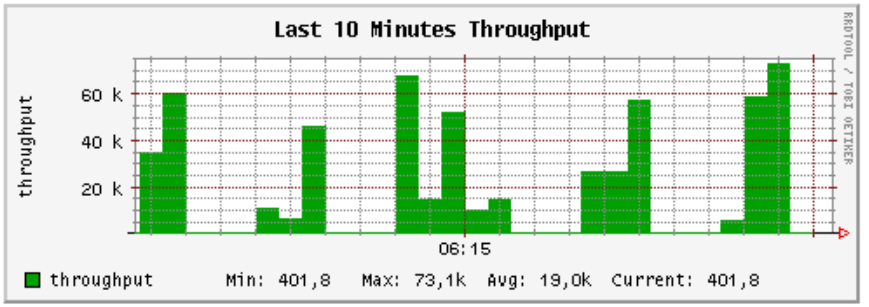
NTOP

Global Traffic Statistics

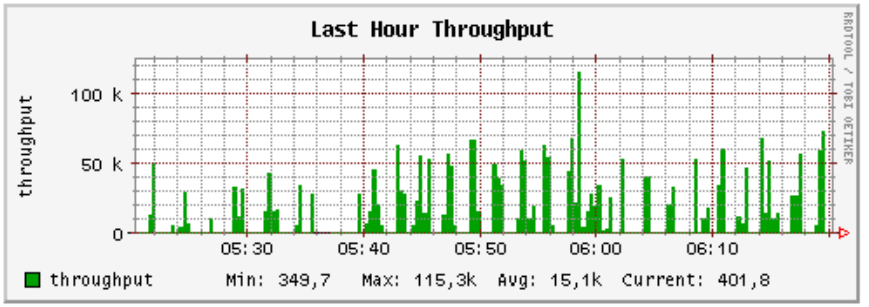
	Name	Device	Type	Speed	Sampling Rate	MTU	Header	Address	IPv6 Addresses
Network Interface(s)	eth0	eth0	Ethernet		0	1514	14	192.168.0.2	::/0
	eth1	eth1	Ethernet		0	1514	14	192.168.1.1	::/0
	eth2	eth2	Ethernet		0	1514	14	192.168.2.1	::/0
	eth3	eth3	Ethernet		0	1514	14	192.168.3.1	::/0
	eth4	eth4	Ethernet		0	1514	14	192.168.4.1	::/0
	eth5	eth5	Ethernet		0	1514	14	192.168.5.1	::/0
	eth6	eth6	Ethernet		0	1514	14	192.168.6.1	::/0
	eth8	eth8	Ethernet		0	1514	14	192.168.8.1	::/0
	eth10	eth10	Ethernet		0	1514	14	192.168.10.2	::/0
	eth11	eth11	Ethernet		0	1514	14	192.168.11.2	::/0
	eth12	eth12	Ethernet		0	1514	14	192.168.12.1	::/0
Local Domain Name	iescopernic.com								
Sampling Since	Mon Nov 19 16:51:51 2007 [7 days 20:25:01]								
Active End Nodes	681								



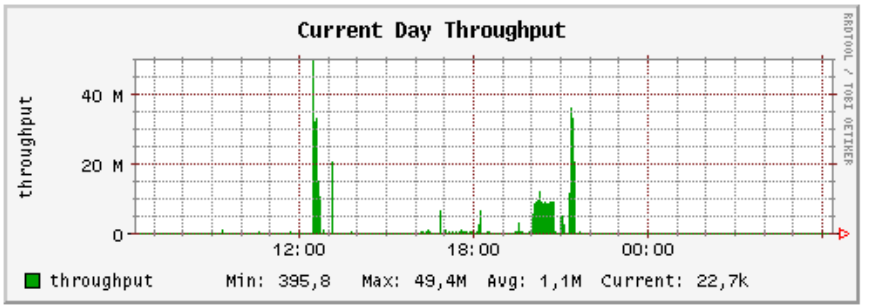
Network Load Statistics



Time [Thu Nov 29 06:10:16 2007 through now]



Time [Thu Nov 29 05:20:16 2007 through now]



Autor: Sergi Tur Badenas

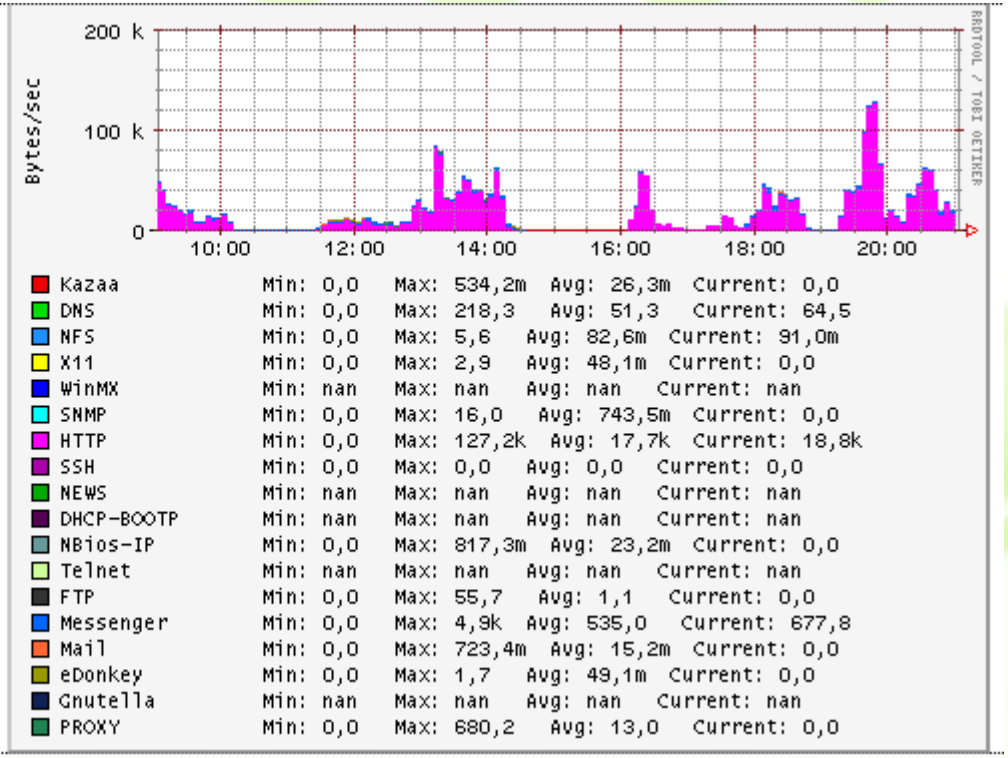
NTOP

Host Information

Traffic Unit: [**Bytes**] [Packets]

Host	Domain	IP Address	MAC Address	Other Name(s)	Bandwidth	Nw Board Vendor	Hops
www.iescopernic.com		192.168.0.7	00:17:08:54:85:87				
192.168.0.2		192.168.0.2	00:30:05:4C:90:1C			Fujitsu Siemens Computers	
192.168.4.2		192.168.4.2					
192.168.0.10		192.168.0.10	00:13:49:87:40:66				
00:19:06:19:73:85			00:19:06:19:73:85				
bridge sp. tree/osi route:00:00:00			01:80:C2:00:00:00			Bridge Sp. Tree/OSI Route	

Historical View



Autor: Sergi Tur Badenas

"Hacking" Tools

- **Network Security Tools**
  - **Auditorías de seguridad**. Detectores de vulnerabilidades como **Nessus** o Nikto.
  - **Benchmarks y test de carga:** Jmeter, siege
  - **Auditoría LAN**
    - Detección de ataques LAN: ARP-Spoofing, ICMP Redirect, Port Stealing, DHCP Spoofing
    - **Ettercap, Dsniff, arpwatch**
  - **Auditoría Wireless LAN (WLAN): Kismet**, aircrack-ng
  - **Detectors de Rootkits**: rkhunter, chkrootkik
  - **Comprovación y mantenimiento de la integridad de un sistema**: debsums, tripwire, integrit, aide, samhain

Autor: Sergi Tur Badenas

Intrusion detection Systems (IDS)

snort1 /snɔ:rt /|| /snɔ:t/ verbo intransitivo
bufar, resoplar verbo transitivo (utter)
bramar, gruñir(conj.⇒)

- **Intrusion Detection System**
  - Sistema de detección de intrusiones
  - Es el estándar “de facto” de sistemas NIDS(Network IDS)
  - Sistema de alertas altamente configurable, basado en detección de patrones de ataques.
  - Dispone de una importante base de datos (libre y comercial) con
  - IDS pasivo (solo detectar) y IDS activo (combinado con iptables, permite realizar acciones frente a ataques detectados).
  - Herramientas extras: ACID, oinkmaster.

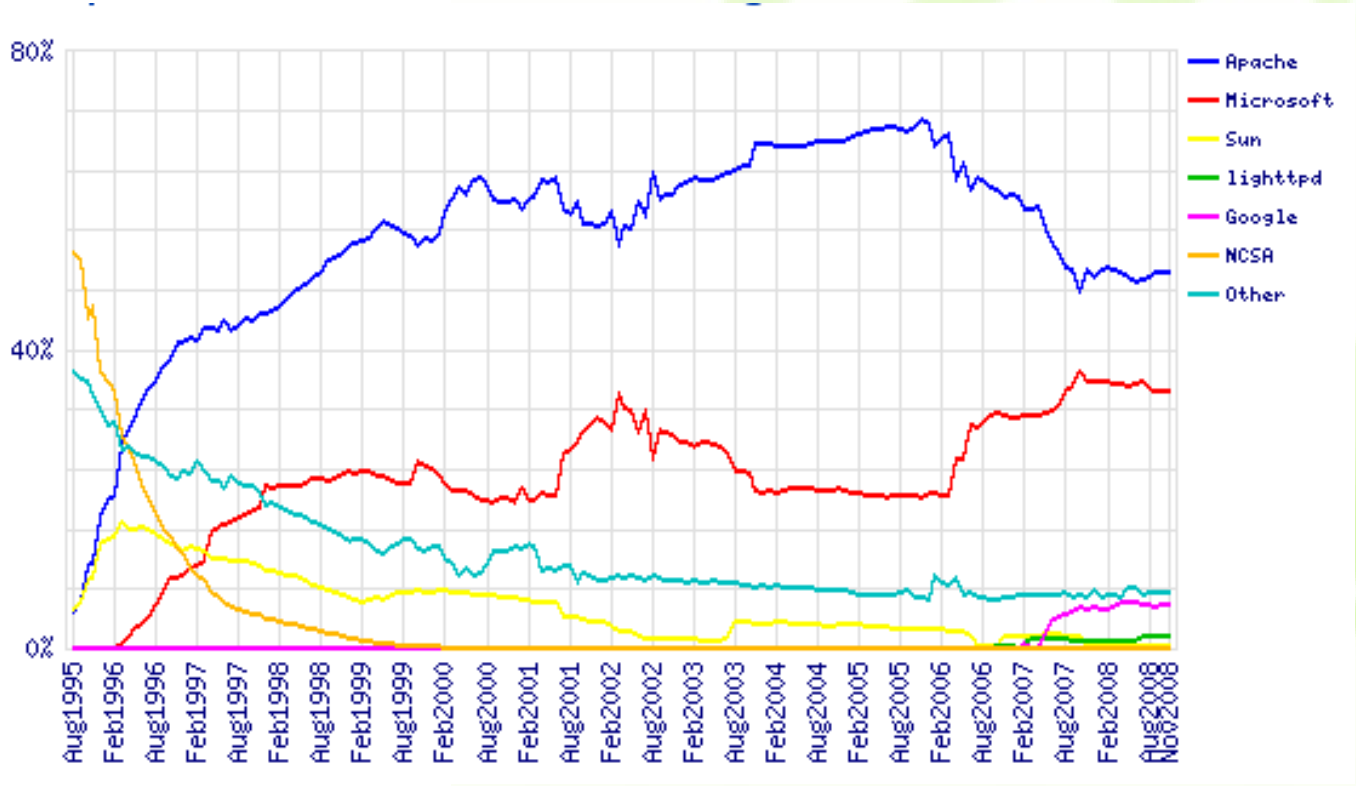
Autor: Sergi Tur Badenas

Servicios de red

Autor: Sergi Tur Badenas

Servidores Web

- **Cuota de mercado servidores web según netcraft**
  - Google Web Server (GWS) basado en Apache
  - ***Lighttpd*** también es *Open Source*



Autor: Sergi Tur Badenas

Servidor Web. Apache

- **Características**
  - Apache License
  - Multiplataforma.
  - Desarrollado el año 1995 a partir del NCSA HTTPd.
  - Mantenido por la Apache Software Foundation.
- **Soporte básico para el desarrollo de aplicaciones web en plataforma LAMP**
  - **L** de Linux, **A** de Apache, **M** de Mysql y **P** de PHP
  - También se utiliza como a plataforma de desarrollo WAMP (Windows AMP)

Autor: Sergi Tur Badenas

Apache Software Foundation

- **Otros proyectos de la ASF:**
  - Jakarta, proyectos Java de servidor:
    - Jakarta Tomcat
    - Jakarta Struts
    - Jakarta-Commons
  - Apache **Ant**
  - Apache **Geronimo**. Servidor de aplicaciones J2EE
  - Apache **XML**. Soluciones XML per a la web
  - Apache **Cocoon**
  - Apache **Lenya** (CMS)
  - Apache **Axis**. Serveis Web
  - **SpamAssassin** - filtre de SPAM

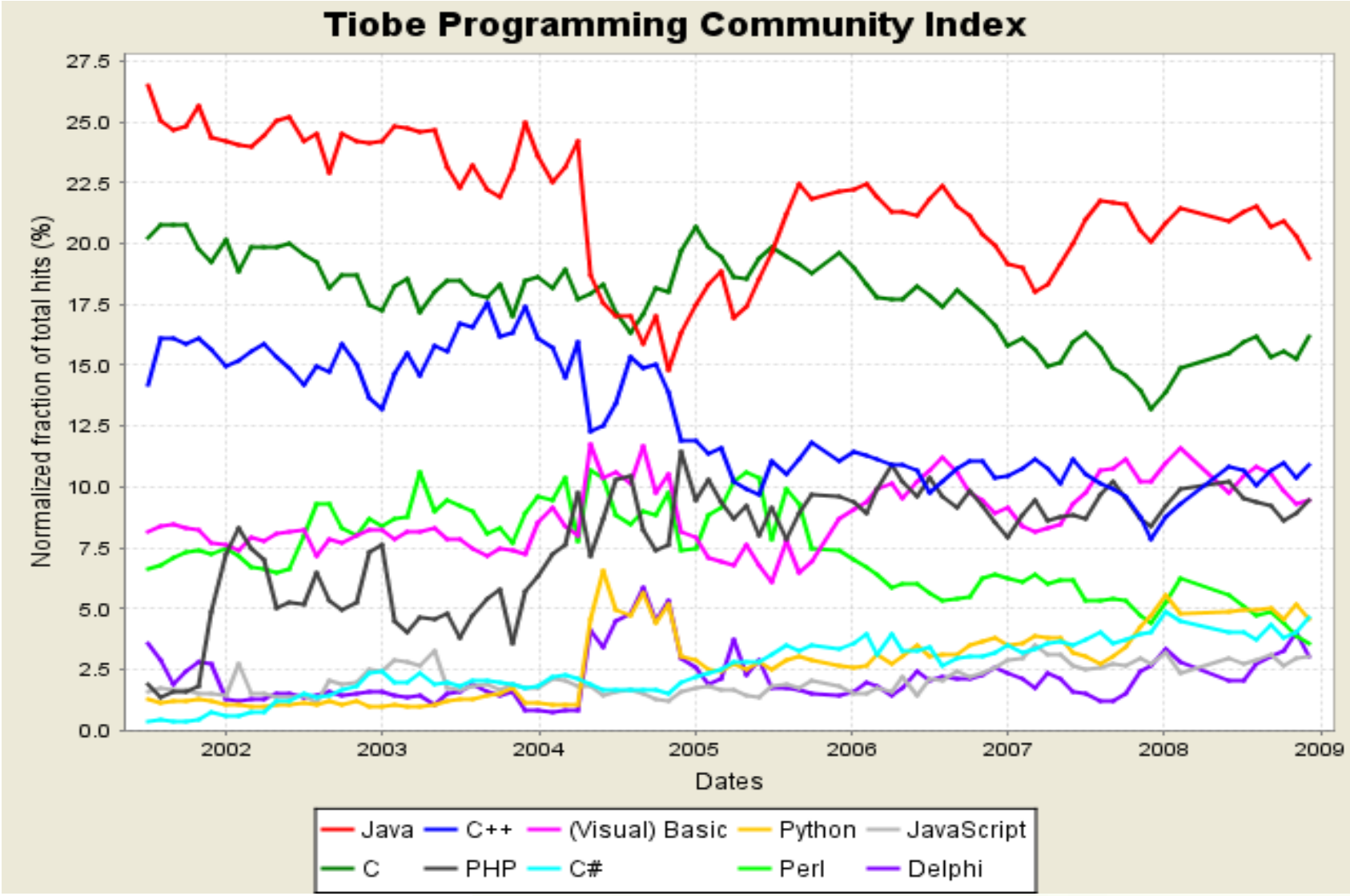
Autor: Sergi Tur Badenas

Servidores de aplicaciones

- **Servidores web + soporte para algún lenguaje o plataforma:**
  - **LAMP o LAPP:** Linux+ Apache+Mysql/PostgreSQL+PHP
    - Fácilmente integrable y con alto rendimiento en Apache
  - **Java**
    - **Apache Tomcat:** Servidor de aplicaciones Java de referencia
  - **Python**
    - **Zope:** Servidor de aplicaciones web basado en Python. Plataforma del CMS Plone
  - **Mono**
    - Proyecto de código abierto (impulsado por Novell) para la creación de herramientas libres, basadas en GNU/Linux y compatibles con .NET
    - Otras tecnologías Open Source: **Ruby On Rails, Perl**, etc...

Autor: Sergi Tur Badenas

Lenguajes de programación

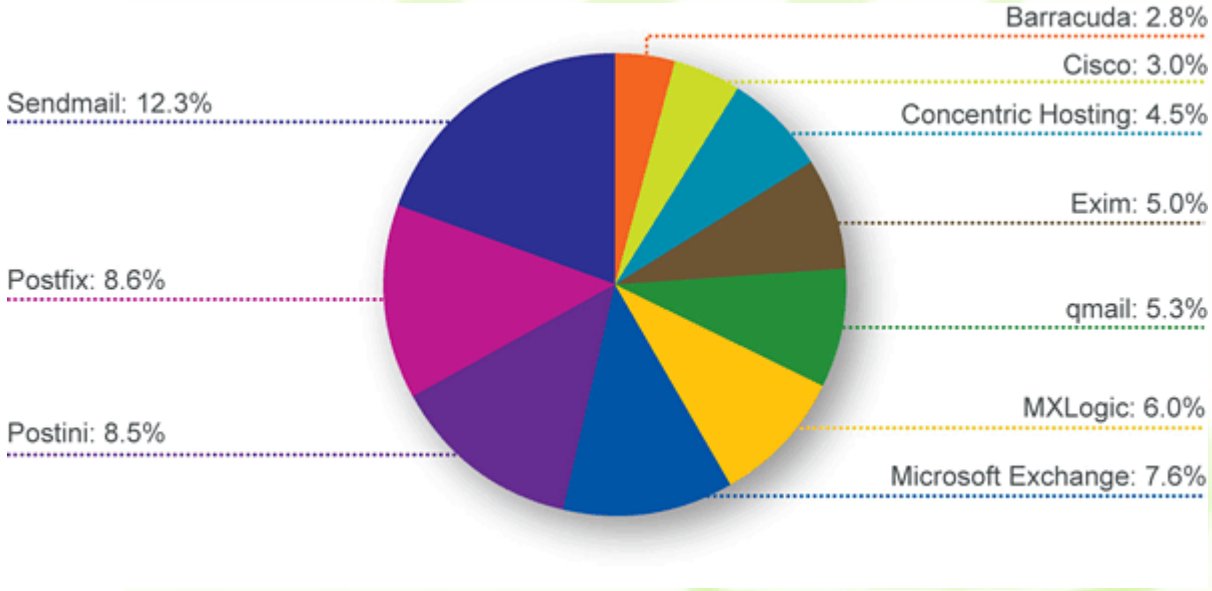


http://www.tiobe.com/index.php/content/paperinfo/tpci/index.html

Autor: Sergi Tur Badenas

Servidores de correo electrónico

- **Cuota de mercado dominada por Open Source**
  - Servidores SMTP
    - Sendmail
    - Postfix
    - Exim
    - Qmail



  - También hay muchas herramientas para los protocolos POP y IMAP. La mas destacable Courier Mail Server

Autor: Sergi Tur Badenas

Sendmail

- **Sendmail**
  - Servidor de correo electrónico más utilizado.
  - Sendmail License, variante de la licencia BSD
  - Creado en 1980 a partir de delivermail d'ARPANET
  - Actualmente esta disminuyendo el uso de Sendmail
  - Muy flexible pero complicado de configurar correctamente.

Autor: Sergi Tur Badenas

Exim

- **Exim (EXperimental Internet Mailer)**
  - Licencia GNU GPL.
  - Creado en 1995 como alternativa a Sendmail.
  - Configuración similar a Sendmail pero vuelto a escribir des de cero pensando en la seguridad.
  - Muy configurable y con funcionalidades extras (listas de control de acceso ACL, antispam, antivirus).
  - Cada vez mas distribuciones lo incorporan por defecto:
    - Ubuntu, Debian o SkoleLinux

Autor: Sergi Tur Badenas

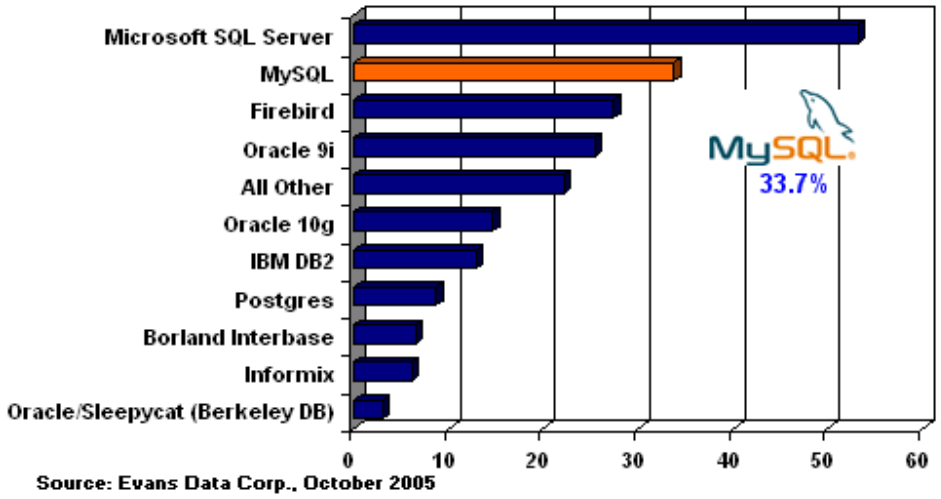
Postfix

- **Postfix**
  - MTA de con licencia IBM Public License incompatible con GPL
  - Creado en 1999 como alternativa a Sendmail.
  - Más fácil de administrar y configurar.
  - Inicialmente conocido como Vmailer o IBM Secure Mailer.
  - Cada vez mas distribuciones lo soportan en detrimento de Sendmail.

Autor: Sergi Tur Badenas

Servidores de bases de datos

- **MySQL**
  - Adquirida por Sun en 2008
  - Es el SGBD con mayor aumento de cuota de mercado de los últimos años.
  - Utilizado por grandes sitios web como Google, Amazon, Digg, flickr, Craigslist, Joomla!, NASA, Nokia, Slashdot, Wikipedia, WordPress, Yahoo
- **PostgreSQL**
  - Una alternativa a tener en cuenta



Autor: Sergi Tur Badenas

OpenLdap

- **Lightweight Directory Access Protocol (LDAP)**
  - No es puramente una base de datos pero si que es un protocolo de accesos a una base de datos relacional
  - **OpenLDAP** es la implementación de software libre mas utilizada
  - Utilizado para almacenar bases de datos jerárquicas como información de cuentas de usuario y recursos de un dominio
  - El objetivo principal es proporcionar de una base de datos y de un protocolo de acceso estándar a la base de datos de autenticación de un sistema.

Autor: Sergi Tur Badenas

Compartición de ficheros

- **Network File System (NFS)**
  - Sistema nativo de Linux **muy eficiente** para la compartición de ficheros en red
  - **Poco configurable** (no tiene control de accesos por usuarios)

- **Samba**
  - Creado por Andrew Tridgell a partir de **ingeniería inversa**
  - Reimplementación de protocolos SMB/CFIS (**redes Windows**):
    - **NetBIOS** over TCP/IP (NetBT), SMB (aka CIFS)
    - **WINS server** (NetBIOS Name Server (NBNS))
    - **Active Directory Logon** (Kerberos y **LDAP**)
    - **Secure Accounts Manager** (SAM) database
  - Permite crear **redes heterogéneas Windows/Linux** con compartición de ficheros y gestión de usuarios en red (dominios Windows).

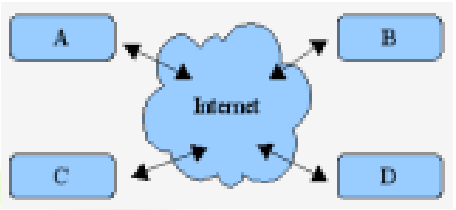
Autor: Sergi Tur Badenas

Samba

- **Funciones de Samba**
  - Servidor de ficheros
  - Servidor de impresoras
  - Servidor DFS de Microsoft
  - Controlador primario de dominio
  - Autenticación Windows 95/98/Me y Windows NT/2000/XP
  - Local & Domain Master Browser.
  - Servidor primario WINS (“DNS” para los nombres de máquinas Windows -Netbios Name-)

Autor: Sergi Tur Badenas

OpenVPN



- **Open Virtual Private Network**
  - Solución de conectividad de redes remota basada en software. Utiliza SSL (Secure Sockets Layer) y VPN
  - Ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente.
  - Resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas EEI 802.11)
  - Soporta balanceo de carga
  - Integrado en firmwares y distribuciones Linux de red
  - Las distribuciones actuales lo soportan de serie y esta integrado en los clientes gestores de red
  - **Multiplataforma:** disponible en Windows.

Autor: Sergi Tur Badenas

Voz IP (Asterisk)

- **Asterisk**
  - Proporciona las funcionalidades de una central telefónica (PBX).
  - Permite llamadas internas a coste 0 o conectar a un proveedor de VoIP, o RDSI tanto básicos como primarios.
  - Buzón de voz, conferencias, IVR, distribución automática de llamadas...
  - Se pueden crear funcionalidades a medida escribiendo un dialplan en el lenguaje de script de Asterisk o añadir módulos en C o en cualquier otro lenguaje de programación.
  - Licencia GPL
  - Soporta los protocolos voIP: pSIP, H.323, IAX y MGCP.

Autor: Sergi Tur Badenas

Herramientas *Open Source*

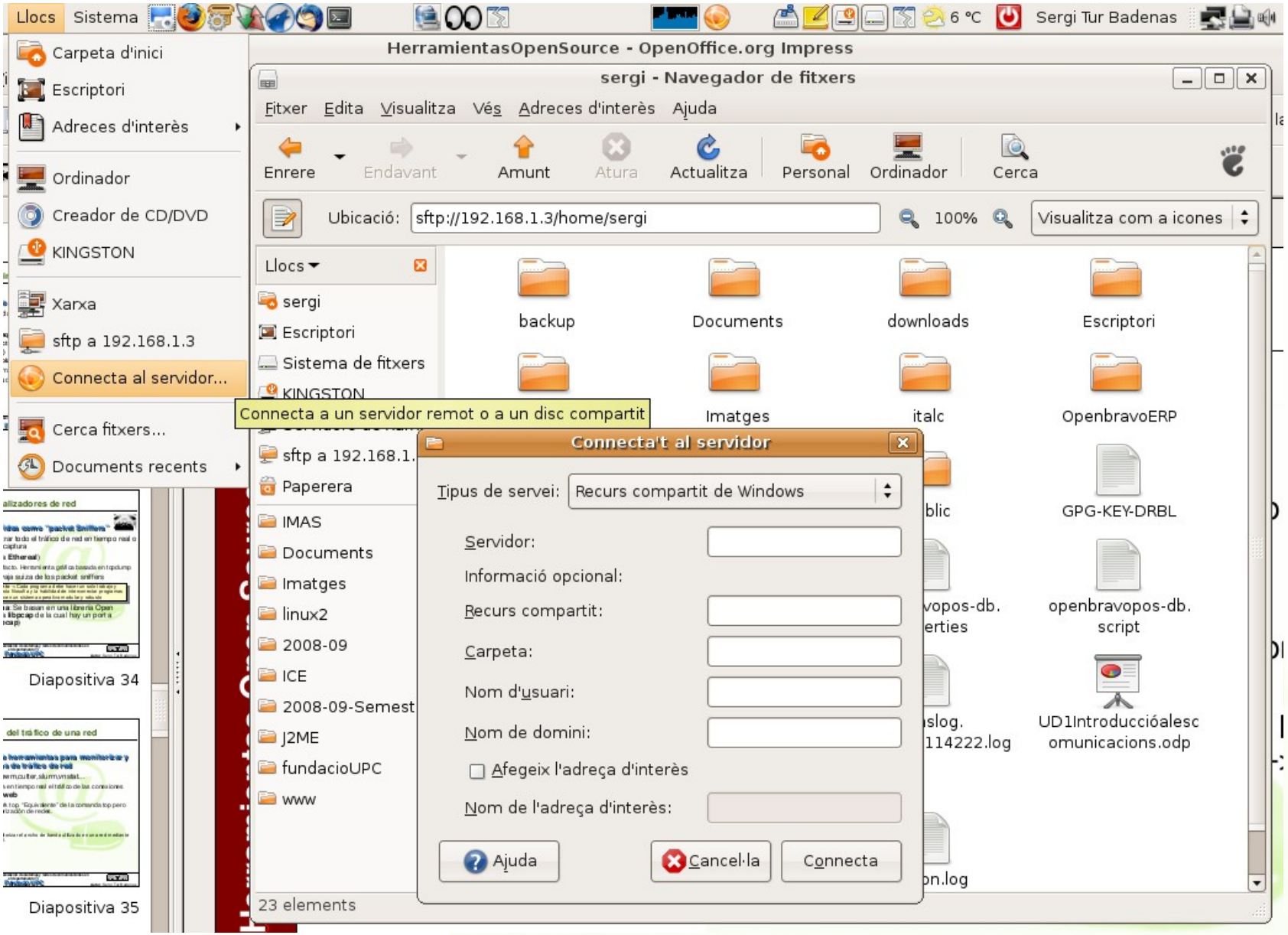
Autor: Sergi Tur Badenas

Gestión remota

- **Acceso remoto a terminal**
  - **Telnet**: No recomendado por razones de seguridad
  - **OpenSSH**: Herramienta más utilizada para el acceso remoto seguro. Permite también SFTP y copia remota (scp).
- **Acceso a escritorio remoto**
  - **VPN**: Hay multitud de clientes VPN. A menudo también soportan conexión remota de escritorio de Windows (**RDP**).
  - **FreeNX**: Alternativa solo para conectar a máquinas remotas Linux (X-Windows). Se comprime el protocolo y no las imágenes --> **velocidades sorprendentes**
- **Transferencia remota de ficheros (backups)**
  - **Rsync:** Copias remotas y locales incrementales
  - **Unison:** Sincronización de carpetas remotas
  - **Rdiff-backup:** Gestión de copias de seguridad incrementales

Autor: Sergi Tur Badenas

Gestión remota



Autor: Sergi Tur Badenas

Terminales “Tontos”. Terminal Server

- **Linux Terminal Server Project (LTSP)**
  - Conjunto de aplicaciones de servidor que permiten ejecutar Linux en computadoras de pocas prestaciones (terminal tonto
  - Se ejecuta el núcleo del sistema a través de la red (boot de red PXE) y los clientes ejecutan aplicaciones gráficas directamente en el servidor utilizando un acceso remoto a escritorio (XDMCP, FreeNX)
  - Muy utilizado en aulas de formación.
  - Bajos costes de mantenimiento de un sistema centralizado. Todo se centraliza en el servidor

Autor: Sergi Tur Badenas

Terminales “Tontos”. Terminal Server

- **Diskless Remote Boot in Linux (DRBL)**
  - Otro sistema para ejecutar distribuciones Linux de forma remota des de la red
  - Basado en NFS y NIS
  - Convierte casi cualquier distribución en una máquina ejecutable de forma remota mediante la carga des de red
  - **Clonezilla:** Herramienta para la clonación de máquinas. Se puede combinar con DRBL para la clonación de máquinas en red mediante UDP multicast

Autor: Sergi Tur Badenas

Virtualización

- **Xen Hypervisor**
  - Desarrollada por la Universidad de Cambridge.
  - Sistema basado en paravirtualización:
    - Mas rápido. Penalización del 2% frente al 20% de los entornos basados en emulación por software
    - No es portable. Cada sistema operativo se debe adaptar, normalmente adaptando el núcleo de Linux
  - Utilizado por ISP para ofrecer servicios de Hosting Virtual
    - Aislamiento seguro
    - Control de recursos
    - Garantías de calidad de servicio
    - Migración de máquinas virtuales en caliente.
    - Alto rendimiento sin un soporte especial de hardware.

Autor: Sergi Tur Badenas

Virtualización

- **Virtual Box**
  - Máquina virtual por emulación de hardware a nivel de software
  - Comprado por Sun en 2008
  - Muy útil como entorno de pruebas
  - Multiplataforma
  - Otras alternativas son qemu, BOCHS o KVM

- **Emulación Windows (Wine)**
  - Es una implementación libre de Windows en Linux. No es 100% fiable pero muchas aplicaciones corren correctamente (en la UPC lo utilizan para ejecutar Lotus Notes)

Autor: Sergi Tur Badenas

Alta disponibilidad

- **The High Availability Linux Project**
  - Provee una solución cluster de alta disponibilidad para Linux, FreeBSD, OpenBSD, Solaris y Mac OS X promoviendo fiabilidad, disponibilidad y servicialidad.
  - La herramienta más conocida es **Heartbeat**
  - http://www.linux-ha.org/
  - KeepAlived: Sistema de redundancia y balance de carga en un *pool* de máquinas **LVS (Linux Virtual Server). Clustering.** Implementa también VRRPD
  - **Ucarp**: otra herramienta de failover
- **Openmosix**
  - Proyecto cerrado en 2008
  - http://en.wikipedia.org/wiki/Openmosix

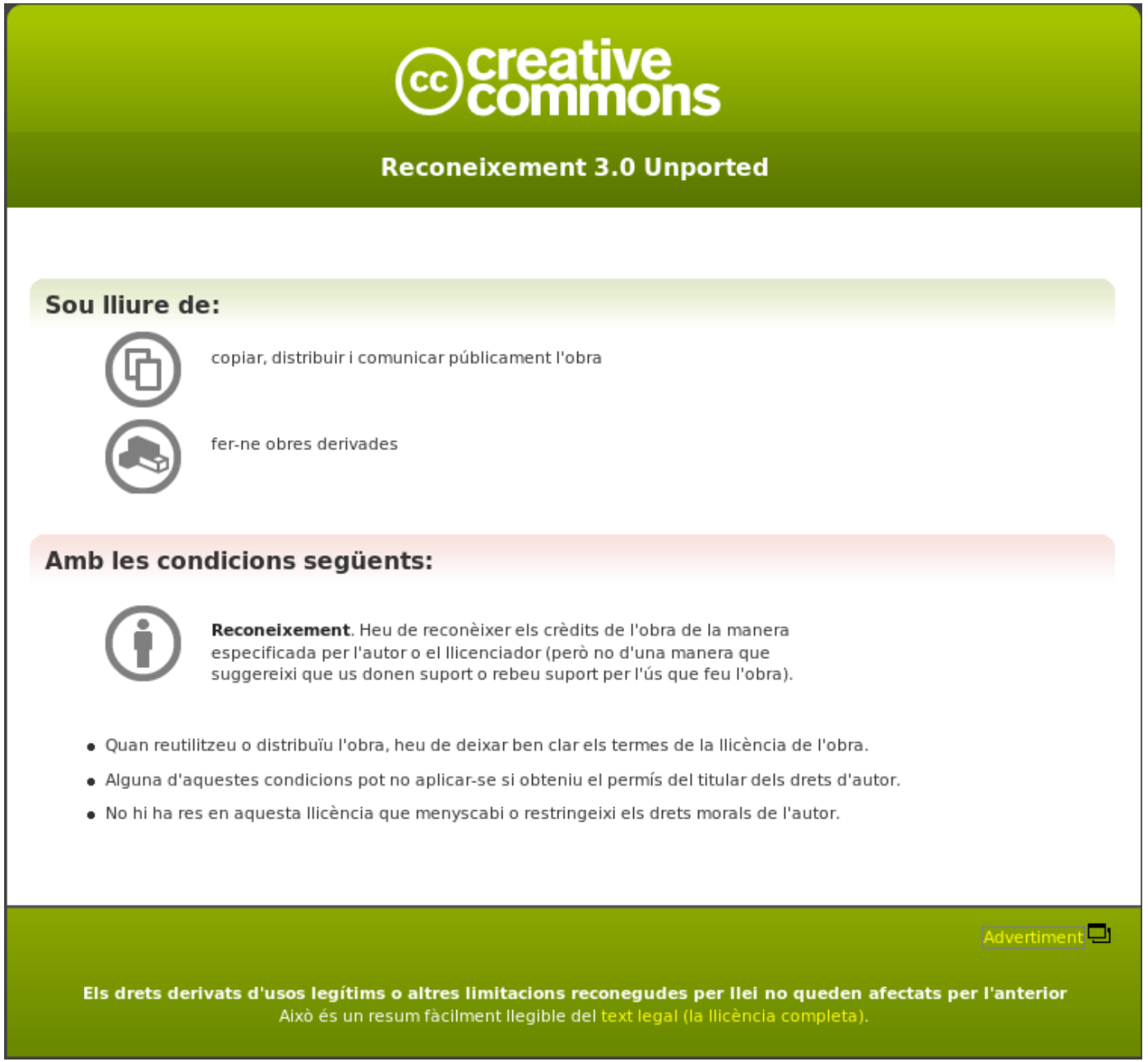
Autor: Sergi Tur Badenas

Más información

- **Curso de Seguridad en redes en formato Moodle**
  - Lo podéis encontrar en el Campus Virtual de l'IES Nicolau Copèrnic
    - http://www.iescopernic.com/moodle
    - Seguretat en xarxes informàtiques
- **Otros cursos en formato Moodle**
    - Cursos Moodle Sergi Tur
- **Documentación en la wiki del ponente**
  - Wiki del ponent

Autor: Sergi Tur Badenas

Llicència Creative Commons



http://creativecommons.org/licenses/by/3.0/deed.ca

Autor: Sergi Tur Badenas