Fundació UPC

Postgrau en Programari Lliure

Assignatura: Administració de Sistemes

1r Capítol: Introducció
2n Capítol: El Projecte Debian
3r Capítol: Usuari
4t Capítol: Administració Local
5è Capítol: Administració de Xarxa
6è Capítol: Apache
7è Capítol: MySQL
8è Capítol: PHP
9è Capítol: LAMP
10è Capítol: Taller

Activitats per capítols
Comandes – Paquets
Bibliografia bàsica
Bibliografia per capítols
Acrònims
GNU Free Documentation License

1r Capítol: Introducció

“Programari Lliure”

- Què és “Programari Lliure”? A quines necessitats respon? Les quatre llibertats[1] de la Free Software Fundation[2] (FSF):
  - *Llibertat 0*: la llibertat per a executar el programa, per a qualsevol propòsit.
  - *Llibertat 1*: la llibertat per a estudiar com funciona el programa, i adaptar-lo a les nostres necessitats. Per tant, tenir accés al codi font esdevé una precondició.
  - *Llibertat 2*: la llibertat per a redistribuir còpies i, per tant, poder ajudar al veí.
  - *Llibertat 3*: la llibertat per a millorar el programa i fer-ne públiques les millores perquè tota la comunitat se'n beneficiï.

    => Llibertat en el sentit de “free speech” i no de “free beer”

    => Cal destacar-ne els fonaments ètics per sobre dels econòmics
- Per a garantir les llibertats anteriors fa falta un instrument jurídic:
  - Genearal Public License[3] (GLP) i projecte de versió 3[4].
  - Les guidelines[5] de la Debian policy[6] van més enllà: permet que l'autor exigeixi que el codi font distribuït no sigui modificat directament sinó que fa que s'hagi d'acompanyar de patchs separats i que es generin binaris amb nom diferent de l'original.
  - Llicències Open Source[7]: Neixen degut a la gran quantitat d'accepcions que té la paraula “free”. N'hi ha d'índole molt diferent[8].
  - -> La llicència[9] Berkeley System Distribution (BSD) no imposa l'accés al codi font. => Estrictament no ho podem considerar com a P. Ll. tot

1 http://www.gnu.org/philosophy/free-sw.html
2 http://www.fsf.org/
3 http://www.gnu.org/copyleft/gpl.html Còpia de la General Public License
4 http://www.fsf.org/news/gplv3 Notícia sobre el procés de redacció de la GLP v.3
5 http://www.debian.org/social_contract.html#guidelines
6 http://www.debian.org/
7 http://opensource.org/licenses
8 De fet entorn del P Ll. i l'open source s'ha obert tota una guerra jurídica.
9 http://www.opensource.org/licenses/bsd-license.html Còpia de la llicència BSD

i que a la pràctica el codi font esdevé quasi bé sempre accessible.

- El Programari Lliure es tradueix en:
  - Millora de la qualitat del codi: seguretat, fiabilitat, suport, etc.
  - Reducció del seu cost: tant de producció com de distribució.

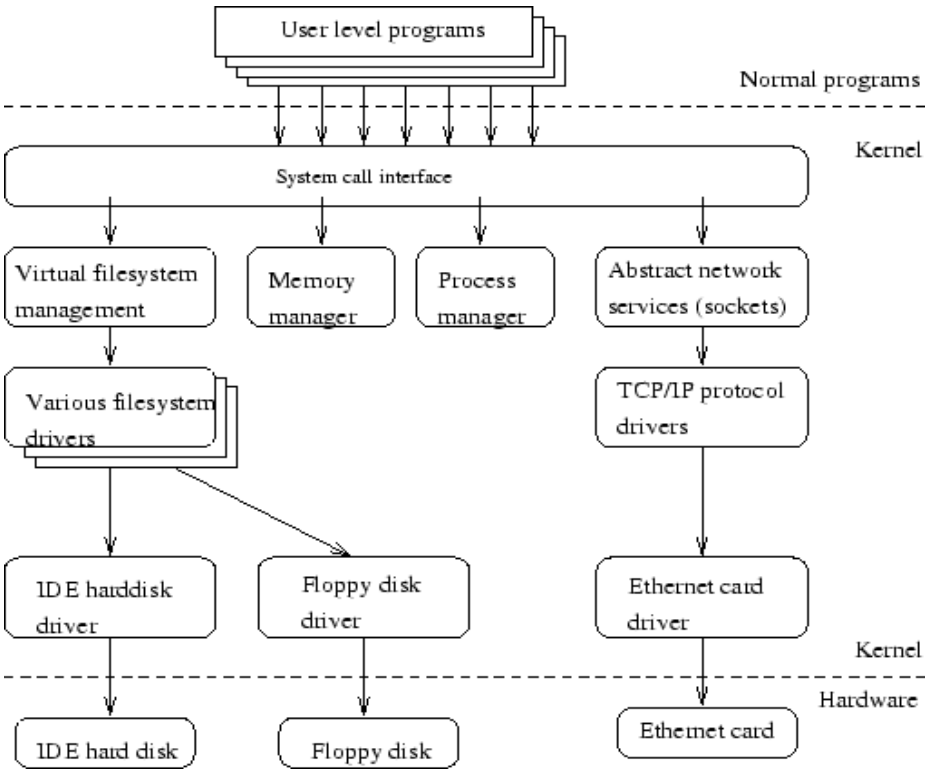
Una mica d'arquitectura

- El nucli (kernel):
  - És el nivell més baix pel que fa a la interacció amb el maquinari
  - Funcions bàsiques:
    - Gestor del sistema d'arrancada del sistema.
    - Gestor de processos: fa possible que un nombre indefinit de processos es puguin executar simultàniament en un nombre finit de CPUs.
    - Gestor de Memòria
    - Sistema de fitxers
    - Gestor de les comunicacions: entre processos
  - És el programari responsable de proporcionar accés al maquinari, i ho ha de fer de manera segura. Els del kernel són els únics processos que s'executen en mode protegit; la resta ho fan en mode usuari.
  - Es mostra a la resta de processos com a un conjunt de funcions de llibreria (System Calls).
  - Tipus de kernels:
    - Monolítics-. Proporcionen una abstracció àmplia i complexa del maquinari
    - Microkernels-. Proporcionen un conjunt reduït d'abstraccions, i es serveixen d'aplicacions addicionals (servers[10]) per a ampliar-ne la funcionalitat.

10 Per exemple la xarxa s'implementa a mode de server, amb el que s'aconsegueix que un error a aquest nivell no pressuposi un bloqueig automàtic del sistema.

- Hibrids o microkernels modificats[11]-. Microkernels que duen incorporat codi extra per a augmentar-ne les capacitats.

- Nuclis oberts de més nomenada:
  - Linux[12]
    - Estructura monolítica modular
    - Implementació unificada (pocs projectes actius, essencialment 2.6 i el 2.4)
    - Multiplataforma
    - El més freqüent en les distribucions
  - Kernel Mach
    - Microkernel
    - alguns projectes que l'usen: BSD, Hurd[13], Mac OSX, etc.



- El programari de sistema operatiu:

11 Per exemple els diferents SO Windows de MS.
12 http://www.kernel.org/
13 http://www.gnu.org/software/hurd.html

- S'executa per sobre del nucli i utilitza les system calls d'aquest per a oferir un joc complet de comandes per a donar utilitat al maquinari.
- Pràcticament tot el codi és de GNU (també per als sistemes BSD).

Font: http://www.gnu.org/graphics/meditate.html .

Gnu lavitant en estat de meditació tocant la flauta.

- Sistema X window (X11R7[14])
  - Arquitectura client-servidor[15]
    - el servidor atén a les peticions del teclat i del ratolí (input) i gestiona la presentació per pantalla (output) per proporcionar suport a les interfícies gràfiques d'usuari[16] (GUI)
    - els clients[17] utilitzen els recursos gràfics del servidor per a presentar els seus resultats
  - Transparent a l'ús en xarxa[18]
    - El servidor[19] sempre s'executa localment[20]
    - els clients són els que “realment fan la feina”[21]

14 Version 11 release 7, aparegut al desembre de 2005; el més utilitzat continua sent el X11R6, aparegut al maig de 1994. El número 11 es refereix a que s'empre el protocol 11 del MIT (1987).
15 L'X Window core protocol estableix les bases per a la interacció entre l'X server i els X clients. L'Xlib és la llibreria resultant de la implementació de l'XW core protocol.
16 Cada GUI corre sobre una instància del servidor; per tant podem tenir més d'una GUI en un ordinador de la mateixa manera que estem acostumats a tenir més d'una consola en mode text.
17 L'ICCCM estableix com els X clients han d'operar sobre un únic X server.
18 Actualment encara no està implementat sobre VNC, però s'hi està treballant.
19 Els servidors X consumeixen molt pocs recursos i es poden executar en qualsevol maquinari que disposi d'una tarja gràfica.
20 Això fa que de vegades hi hagi malentesos, ja de forma inconscient tendim a associar servidor amb execució remota.
21 Els clients X poden ser programes que requereixin molt maquinari, imaginem un generador

        - Els clients es poden executar de forma remota, sobre maquinari molt més potent
        - La variable d'entorn $DISPLAY[22] és la que indica als clients cap a on han de dirigir les seves sortides per a trobar el servidor receptor[23]
    - No estableix cap especificació d'aplicació d'interfície d'usuari[24]. És el software d'usuari[25] l'encarregat d'establir aquest nivell de detall.
    - Widget/GUI toolkits[26]
        - Conjunts d'elements bàsics[27] per a les GUI
    - Xfree86 / X.org
        - Actualment la de la X.org s'utilitza com a implementació canònica de les X. Fins al 2004 havia estat la de la XFree86
- Per sobre de les X[28]
    - Arquitectura clàssica
        - Display managers[29]
            - Gestors d'inici de sessió[30]

---

de fractals, i per tant té sentit que s'executin sobre màquines molt potents.

22 DISPLAY=hostname:displaynumber.sceennumber (man X)
DISPLAY=:0.0 indica que el servidor a qui s'ha d'enviar les sortides està en local i que s'ha d'enviar a la primera pantalla (segon 0) de la primera instància (primer 0).
DISPLAY=192.168.0.3:0.1 indica que el servidor està a la màquina 192.168.0.3

23 El procediment a seguir per a una sessió remota d'X és el següent:
1er-. Engegar el servidor (startx) el qual engegarà un client window manager.
2on-. Des del window manager s'engega un terminal de finestra
3er-. Des del terminal de finestra iniciem la sessió remota (telnet, ssh)
4rt-. Un cop estem a la màquina remota establim el valor de la variable DISPAL (export $DISPLAY=adreça.màquina.local:0.0)
5uè-. En la màquina remota executem el programa client
Nota: Cal assegurar-nos que el sistema servidor X accepta connexions remotes.

24 Això és el que ha permès que les “interfícies” X hagin evolucionat tant al llarg del temps.

25 Window managers, widget toolkits, desktop environments.

26 N'hi ha de basats en Intrinsits (o Xt, llibreria que utilitza l'Xlib per a proporcionar una API OO per desenvolupar widgets) com Xaw (del projecte Athena), Motif (l'utilitzat per CDE), Lesstif (una versió LGPL de Motif), i n'hi ha que utilitzen l'Xlib directament com GTK+ (utilitzat per GNOME) o Qt (utilitzat per KDE, han anat evolucionant en el tipus de llicència).

27 En forma de llibreries o de l'application frameworks.

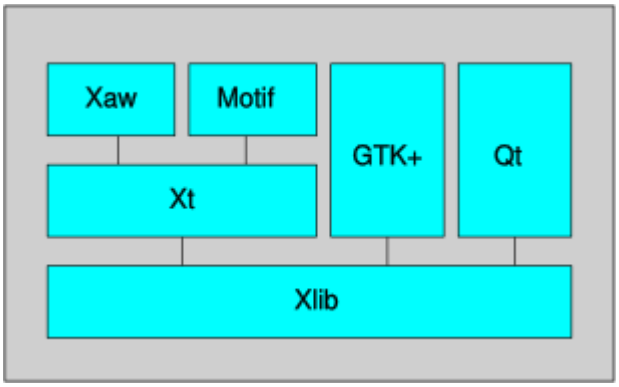
28 http://www.plig.org/xwinman/ Informació sobre window managers i desktop managers

29 xdm (l'original de les X), gdm (de GNOME), wdm (de WindoMaker), etc.

30 Com login o getty per a sessions de text.

- Window managers[31]
  - Controlen l'emplaçament i l'aparença amb què es presenten les finestres.
- Session managers[32]
  - gestionen (engegada, aturada, configuració, etc.) les sessions d'usuaris.

- Entorns d'escriptori (Desktop environments)
  - neixen amb l'objectiu d'oferir una GUI completa: WM, temes, programes i llibreries.
  - GNOME, KDE, CDE[33], Xfce, etc.



Font: http://en.wikipedia.org/wiki/Image:X-client-libraries.svg .

Ús de les Xlib

Distribucions

El concepte de distribució neix de la necessitat d'agrupar programari per tal d'aconseguir una interfície operativa per a poder-hi treballar. Els components mínims d'aquesta agrupació seran, doncs, un nucli (Linux o BSD), i un conjunt d'eines d'administració, generalment procedents de GNU (GNU userland[34]). A més a més, quasi bé totes les distribucions tenen un sistema de gestió de

31 N'hi ha moltíssims, els quals responen a diferents necessitats i plantejaments: xwm (provablement el primer, 1985, anterior a l'X11), twm (escrit directament sobre la Xlib C interface, no utilitza cap toolkit ni widget; el primer ICCCM-compilant, ha deixat una forta empremta sobre molts dels WM posteriors; durant molt temps va ser l'únic WM existent), FVWM, FVWM95, fvwm2, AfterStep, NEXTSTEP, Enlightment, WindowMaker, IceWM, Blackbox, Fluxbox, Metacity, etc.
32 xsm
33 L'estàndard de UNIX
34 http://www.gnu.org

paquets per a facilitar l'administració de programari del nostre sistema.

El fet que Linux hagi estat portat a una infinitat de dispositius fora del seu entorn nadiu, el 0x86, i que, des d'un temps ençà, construir una distribució hagi esdevingut una tasca força senzilla ha fet que actualment hi hagi moltíssimes distribucions disponibles.

Tot això fa que quan ens enfrontem en un problema nou, per triar quina és la millor solució (distribució) per una situació específica i concreta, hàgim de considerar tot un seguit de punts[35], la resposta als quals ens durà cap a una o altra solució. Els punts principals a tenir en compta són els següents:

- **Plataforma**-. Actualment les distribucions més importants han estat portades a moltes plataformes. De fet aquest criteri només esdevé significatiu quan el maquinari és poc estàndard (sistemes de grans prestacions, embeddeds, etc.)

- **Llicències**-. Ja sigui per motius ètics o d'altres, cal anar sempre amb molt de compte amb aquesta qüestió tant a l'hora de seleccionar una distribució com a l'hora d'instal·lar programari de tercers, ja que el sistema de llicències no és tant senzill com el que s'ha presentat anteriorment[36]. Cal parar esment especial a les llicències dels device drivers, llibreries, dependències, etc.

- **Sistema de gestió de paquets**-. El seu objectiu és facilitar la tasca d'administració del programari del sistema. Tots en permeten la seva administració (instal·lació, desinstal·lació i actualització), i els més avançats també gestionen les seves dependències d'altres paquets (consistència, incompatibilitat, etc.). Normalment tant són útils per a la instal·lació de codi font com de binaris. Els més coneguts són:

  - El de Debian: Arxius .deb.
    És un sistema molt robust i per a molts és una referència. Gestiona, de forma molt eficient, dependències i incompatibilitats. També té en compte el tipus de llicències.

  - El de RedHat: Arxius .rpm.
    Donada la gran difusió d'aquesta distribució és el sistema utilitzat per a molts productors de programari. Gestiona correctament les dependències; tot i això no es considera tant potent com el de Debian.

  - El de Slackware: Arxius .tgz (no s'han de confondre amb els tar.gz). No gestiona dependències. És el sistema més senzill dels tots els presentats fins ara.

35 http://en.wikipedia.org/wiki/Linux_distribution#Choosing_A_Linux_Distribution i http://en.wikipedia.org/wiki/Comparison_of_Linux_distributions

36 http://opensource.org/licenses Unes quantes llicències de codi obert

- El de Gentoo: Portage
  No es tracta d'un sistema de paquets literalment, sinó un conjunt d'scripts que faciliten la instal·lació del sistema. És una forma radicalment diferent de plantejar l'administració de paquets de les que s'han vist fins ara.

.deb <--> .rpm: hi ha aplicacions que permeten passar paquets d'un sistema a l'altre i viceversa[37].

També es poden instal·lar paquets manualment i de forma independent al sistema de gestió de paquets de la distribució, però el que es recomana és que si és possible s'utilitzin les eines adients per per integrar-los dins del sistema de paquets.

- **Interfície d'instal·lació**-. Hem de tenir present que la automatització i simplificació de tasques sempre va en detriment de la capacitat d'adaptació del sistema a les nostres necessitats específiques. Cal, doncs, assegurar-se sempre, abans de començar una instal·lació, que durant aquest procés podrem fer allò que ens interessa.

- **Programari**-. També és important saber quina proporció del programari que sabem que necessitarem està dins de la pròpia distribució, i quin l'haurem d'instal·lar des de zero (més dificultats i més temps).

- **Suport extern**-. Quan hi ha involucrats interessos econòmics es pot considerar el fet de la contractació d'un servei de suport extern (un 24/7 per exemple) per a generar confiança.

Com ja s'ha dit, actualment hi ha moltíssimes distribucions disponibles; és per això que s'anima al lector a provar-ne unes quantes per disposar de criteris pràctics de selecció. Es considera que com a mínim caldria haver instal·lat i provat les distribucions que s'esmenten a continuació abans de prendre una decisió.

Algunes distribucions

Debian: Distribució fet íntegrament per voluntaris que formen una comunitat especialment activa. Especialment sensible al fet del programari lliure (Debian social contract[38]). És la que, probablement, disposa de més programari integrat. És la més present als àmbits d'estudi i de recerca.

Geento: Qualsevol instal·lació es fa sempre a partir de la compilació del codi font. Això fa que es tregui molt rendiment del maquinari disponible. Tot i que és relativament jove en el temps, és molt activa. És considerada la més complicada d'instal·lar i per això és, probablement, amb la que s'aprèn més.

37 De .rpm a .deb es pot fer amb alien.
38 http://www.debian.org/social_contract

Fedora Core: Projecte esponsoritzat per Red Hat, només conté programari obert, utilitza el sistema de paquets RPM. És necessari conèixer aquesta distribució ja que és la que s'utilitza més en l'àmbit empreserial.

Ubuntu: Distribució basada en Debian, està fortament marcada per la seva filosofia; apareguda recentment, ha estat, sens dubte, la que ha tingut el gradient més gran d'usuaris, els quals han generat, en els seus fòrums, gran quantitat de documentació. S'utilitza sovint com a punt de partida per a noves distribucions. També es distribueix en forma de liveCD[39].

Ututo-e: Distribució que es nodreix exclusivament de programari lliure[40]. Orientada a escriptori.

Suse: Distribució que es caracteritza per la incorporació d'una eina que pretén centralitzar totes les tasques de l'administrador de sistemes (YaST2), utilitza, per sota el sistema de paquets RPM. Aquesta distribució ha tingut els seus dalt i baixos, però actualment sembla que gaudeix de bona salut.

Mandriva: Els esforços de molta gent han fet que, aquest producte de diverses fusions empresarials, tingui una quota d'usuaris respectable. Utilitza el sistema de paquets RPM.

Slackware: És considerada la “primera” distribució de GNU/Linux cronològicament parlant. Actualment manté l'activitat. El sistema de paquets és força primitiu.

Altres distribucions han optat per a la tecnologia BSD. De codi obert essencialment n'hi ha tres[41]: FreeBSD[42] (amb una quota de mercat del 80%), NetBSD[43] i OpenBSD[44].

També cal destacar la tasca pels membres del projecte Debian GNU/kFreeBSD la distribució sobre un nucli BSD, el qual ja és una realitat dins versió inestable de la distribució.

Una mica d'història

A grans trets	
1960-1970	El software és intrínsecament lliure; de fet no es concep, des de cap punt de vista, el vendre hardware sense el seu software corresponent, el qual generalment es facilita en forma de codi

39 Sistema operatiu emmagatzemat en un CD el qual es pot utilitzar com a sistema d'arrancada i que es caracteritza per no deixar rastre en el sistema sobre el que s'executa, ja que totes les operacions d'escriptura es fan sobre memòria d'accés aleatori.
40 De fet Richard Stallman, octubre 2005: “But the only free GNU/Linux I know of is UTUTO”
41 El codi del nucli del sistema operatiu Mac OS X, alies Darwin, també és obert
42 http://www.freebsd.org/
43 http://www.netbsd.org/
44 http://www.openbsd.org/

A grans trets	
	font.
1970-1980	El desenvolupament de programari va totalment lligat al model econòmic del programari propietari. Les poques iniciatives que actualment podríem associar al moviment del P. Ll. tenen força problemes per falta de fonaments legals[45].
1980-1990	Naixement del moviment del P. Ll. tal i com el coneixem avui. Richard Stallman posa en funcionament el GNU i crea la FSF per a donar-li recolzament. Així mateix, mitjançant la GLP, posa els fonaments legals per evitar que mai més un codi públic pugui privatitzar-se.
1990-2000	Dècada de l'expansió del P. Ll. L'aparició de Linux facilita l'aparició de les primeres distribucions GNU/Linux, i aquestes fan possible que el seu ús es faci extensiu molt més enllà dels entorns universitaris, a on, fins llavors, havia estat pràcticament restringit. La filosofia i l'ètica del P. Ll. s'exporta a altres disciplines fora del món de la informàtica[46].
2000-...	El P. Ll. és, en molts entorns, el paradigma inqüestionable de desenvolupament i d'ús del programari.

Amb una mica més de detall[47]	
1969	IBM, industria dominant en el sector informàtic, anuncia que a partir de mitjan 1970 començarà a vendre el software de forma independent al hardware: neix la industria del software propietari tal i com la coneixem avui.
1970	Als laboratoris Bell Labs de l'empresa AT&T s'inicia el desenvolupament del sistema operatiu UNIX[48] (Thompson i Ritchie). Tot i que cal tenir la llicència d'AT&T per utilitzar-lo, la companyia facilita el codi font a tot aquella entitat que el vulgui per estudiar-lo; això fa que l'ús d'aquest SO s'estengui per moltes universitats, especialment entorn del CSRG[49],convertint-se en el SO per excel·lència en els àmbits docents i d'investigació.

45 És especialment representatiu el cas del conflicte entre AT&T i la Universitat de Califòrnia, el qual va acabar als tribunals al 1991. La causa era que el CSRG havia publicat codi que s'havia produït dins del propi grup però que estava sota llicència d'AT&T, ja que aquesta era necessària per a treballar amb UNIX.
Hi ha qui veu, en aquest embolic legal, la raó fonamental per la qual el kernel de BSD ha tingut una difusió menor que el Linux, essent aquest últim posterior en aparèixer cronològicament.

46 Apareixen les llicències Creative Commons, etc.

47 http://eu.conecta.it/paper/Some_dates_open_source.html

48 Filosofia UNIX: el sistema de comandes format per moltes aplicacions petites, cadascuna de les quals només fa una tasca, però que la faci el millor possible; aquestes aplicacions s'invocaran des de scripts (seqüencies de comandes dins d'estructures de programació) per a constituir aplicacions més complexes, que són presentades a l'usuari final.

49 Computers Science Research Group, Universitat de Califòrnia, Berkeley

Amb una mica més de detall	
1983	Manifesto[50] de Richard Stallman.
1984	Fundació de GNU. Richard Stallman abandona el MIT[51] per dedicar-se exclusivament al projecte GNU. Els primers objectius inicial són el desenvolupament d'un compilador (GCC) i d'un editor de text (Emacs). L'objectiu final: l'obtenció d'un sistema de programari complet de propostit general totalment lliure.
1985	El MIT base X Consistorium distribueix el sistema X Window amb codi obert.
1985	Richard Stallman crea la FSF.
1989	El CSRG allibera, amb llicència BSD, la part del codi de UNIX que ha produït relacionada amb TCP/IP (implantació al kernel i utilitats; Net-1).
1990	La FSF inicia el projecte Hurd. La recerca en SO prediu l'extinció dels kernels molítics.
1991	Linus Torvalds fa pública la versió 0.01 de Linux
1992	Primera distribució GNU/Linux que incorpora elements com les X o suport TCP/IP.
1993	Ian Murdock comença el projecte Debian GNU/Linux.
1994	Linux 1.0
1996	Linux 2.0
1998	Netscape publica gran part del codi de Navigator[52].
1999	Linux 2.2 / Apple allibera Darwin.
2000	Mozilla M13
2001	Linux 2.4
2002	OpenOffice 1.0

Models de desenvolupament: el model catedral i el model bazar[53]

- Model catedral
  - pocs desenvolupadors organitzats piramidalment

50 http://www.gnu.org/gnu/manifesto/.html
51 Massachusetts Institute of Technology
52 Durant aquest procés es forja el terme “open source” en reacció al terme “free software” de Richard Stallman
53 Aquests models foren identificats i batejats per Eric Steven Raymond i descrits en el seu article “The Cathedral & the Baazar”, maig 1997, http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/

    - poques beta espaiades en el temps
    - a l'usuari, purament consumidor, li ha d'arribar versions lliures d'errors i finalitzades
    - exemples: FSF
- Model basar
    - organització pràcticament horitzontal
    - pot ser desenvolupador qualsevol que sigui capaç de fer patches
    - es van traient versions constantment (habitualment estable/desenvolupament)
    - informació pública del que s'està fent
    - l'usuari esdevé un element actiu en el projecte (feedback)
    - exemples: Linux

2n Capítol: El projecte Debian

Introducció

- Característiques principals:
    - estabilitat[54]
    - robustesa en les eines d'administració
    - fiabilitat
- 11 plataformes suportades[55]: Alpha, ARM, HP PA-RISC, Intel x86, Intel IA-64, Motorola 680x0, MIPS, MIPS (DEC), PowerPC, IBM s/390, SPARC
    - Es persegueix la unificació màxima de la funcionalitat i aparença entre les diferents plataformes (quedant-ne exclosa la gestió dels processos d'engegada, degut a les diferències arquitectòniques).
- Més de 15.400 paquets llestos per a ser instal·lats i utilitzats
- Es procura que el programari empaquetat sigui el més semblant possible al de les fonts originals:
    - No s'hi afegeixen canvis substancials.
    - Es vol garantir que entri a formar part del sistema integrat sense conflictes.
    - Si en el procés de “debianització” es produeixen modificacions no específiques de Debian, s'intenta que aquestes entrin a formar part del upstream code.
- Té un compromís molt fort amb la comunitat del free software.
    - Reciprocitat: Tot el seu treball es fa disponible a la resta de la comunitat, de la mateixa manera que s'adobten les millores externes en benefici propi.
    - Molt sovint les millores aportades són adoptades per altres distros.

54 Entesa en el sentit del manteniment de versions en el temps; no en el sentit absència de fallides en el programari, ja que això és responsabilitat de cada projecte en particular, i des de Debian s'entén que cadascú fa la seva feina ben feta.

55 Web: http://www.debian.org/ports/

- La comunitat Debian està formada exclusivament per voluntaris:
  - Tots els membres abans de ser acceptats oficialment com a tals han de demostrar un fort compromis amb la comunitat
  - La filosofia, l prestigi social que té pertànyer a la comunitat i el nivell tècnic que mostra atrau professionals d'arreu del món.
  - Es regeix per un sistema meritocràtic.

    => Se'n pretén garantir la neutralitat comercial
- L'objectiu principal de la política de “nous usuaris” és que aquests quedin satisfets de la decisió d'adherir-se a l'ús de Debian.

  => mai es presenta la informació de forma “panfletària”, sinó que sempre es busca la màxima transparència i objectivitat

El projecte Debian

Una mica d'història[56]	
1993	A l'agost Ian Murdock[57] proposa públicament[58] la creació i manteniment d'una distro seguint el model descentralitzat de Linux[59]; de seguida rep força adhesions. En un article al Linux Jurnal[60] exposa les idees principals que fonamentaran el Debian Manifesto[61].
1994	Al gener apareix la primera release pública, la Debian 0.91. Ian Jackson es posa a treballar en el dpkg[62].
1995	La 0.93R6 incorpora el dselect.
1996	Bruce Perens redacta: • el Debian Social Contract[63], per definir idees i prioritats del projecte, • i les Debian Free Software Guidelines[64] (DFSG), a on defineix els criteris que el programari ha de tenir per assolir la qualitat necessària per a entrar a formar part del projecte. • També impulsa la creació de l'entitat Software in the Public

56 Podeu trobar aquesta informació i molta més al paquet debian-history.
57 Fins a les hores havia estat usuari de SLS (Softlanding Linux System, Peter MacDonald, mig 1992); però el canvi en aquesta distro de a.out a ELF el va contrariar. Cal esperar fins a 1996 que no s'incorpori el format ELF per a l'arquitectura i386.
58 Web: http://lists.debian.org/debian-devel-announce/2003/08/msg00008.html
59 El que ara es denominaria model bazar, segons la proposta de E. Raymond.
60 Web: http://www.linuxjournal.com/node/2841
61 Web http://www.debian.org/doc/manuals/project-history/ap-manifesto.en.html
62 Debian package management system
63 Web http://www.debian.org/social_contract
64 Web http://www.debian.org/social_contract#guidelines

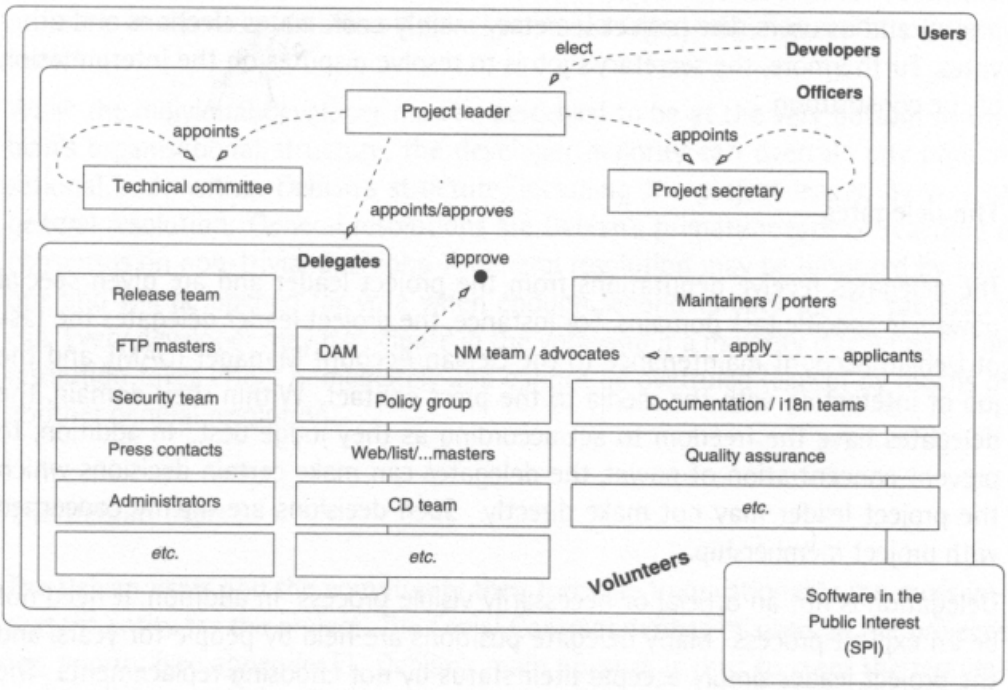
Una mica d'història	
	Interest per a donar suport legal a aquelles parts del projecte que ho requereixen (registre de marques, finançament, etc.)
1999	La 2.1 incorpora l'apt[65].

Unes quantes dades				
Any	Project Leader	Desenolupadors	Packets	Releases
1993	Ian Murdock			
1994		12		0.91
1995		60		0.93R3
1996	Bruce Perens	120	474 848	1.1[66] “buzz” 1.2 “rex”
1997		200	974	1.3 “bo”
1998	Ian Jackson	400	1500	2.0 “hamm”
1999	Wicher Akkerman		2250	2.1 “slink”
2000		450	4000	2.2 “potato”
2001	Ben Collins			
2002	Bdale Gardee	900	9000	3.0 “woody”
2003	Martin Michmayr			
2004				
2005	Branden Robinson	1600	15400	3.1 “sarge”

Organitzacions de les que forma part	
FSG	Free Standards Group
LSB	Linux Standard Base[67]
FHS	File Hierarchy System

65 Advanced package tool.
66 La release 1.0 mai es va distribuir degut a un error d'etiquetatge a l'impressió del CDROM.
67 Paquets lsb, lsbdev i debian-lsb.

La comunitat Debian



Els documents fonamentals de Debian

Debian Social Contract:

1. Debian will remain 100% free
2. We will give back to the free software community
3. We will not hide problems
4. Our priorities are our users and free software
5. Works that do not meet our free software standards

Debian Free Software Guidelines:

1. Free Redistribution
2. Source Code
3. Derived Works
4. Integrity of The Author's Source Code
5. No Discrimination Against Persons or Groups
6. No Discrimination Against Fields of Endeavor
7. Distribution of License
8. License Must Not Be Specific to Debian
9. License Must Not Contaminate Other Software
10. Example Licenses

Debian Manifesto:

1. What is Debian Linux?
2. Why is Debian being constructed?
3. How will Debian attempt to put an end to these problems?

Debian Policy Manual

- És el document tècnic de referència per als desenvolupadors de Debian.

Fonaments teòrics

Tipus de paquets

- El conjunt de paquets de Debian formen el que es coneix com a Debian software pool.

Seccions de pool	
main	Conté el programari que compleix integrament les DFSG. Els paquets només poden dependre d'altres paquets de main. • Constitueix un 97% de tot el software de Debian. • Els esforços més importants del projecte es centren en la millora i manteniment d'aquesta secció.
contrib[68]	Els seus paquets, tot ser software lliure, depenen d'altres que són contrib o non-free. Poden dependre d'altre programari que no pot ser empaquetat. • No són activament soportats. • No són competència del grup de seguretat.
non-free	Els seus paquets no compleixen les DFSG. • No tenen suport oficial.

A /usr/share/doc/<pacakgename>/copyright hi ha una còpia de les disposicions legals amb què es distribueix cada paquet.

68 Gran part del programari (drivers) per donar soport a maquinari que no està inclòs directament a dins del kernel pertany a aquest grup, ja que sovint depèn d'alguns fracments de codi (firmware habitualment) que està al non-free per problemes de llicències.

Tipus de paquets segons el seu contingut	
binary	Contenen programari compilat i preparat per a ser instal·lat amb les eines de gestió de paquets de Debian. Es caracteritzen per la extensió .deb. Es pot donar el cas que, per qüestions de dependències, estiguin buits[69].
source	Són paquets formats per dos o tres fitxers. Aquests fitxers junts contenen tot el necessari perquè els scripts del mantenidor del paquet puguin generar els paquets binaris. Un paquet de fonts, conté, per tant, tot el codi del programari i tot el codi necessari per a generar els binaris a partir del codi de programari[70].

Releases

- Surten quan “they are ready”.
- La qualitat és la màxima prioritat del projecte.
- En cap moment responen a estratègies de mercat.

Estats del programari[71] (official releases)	
unstable	• Primer estadi dins del cicle de vida d'un paquet. • Es pretén que cada paquet contingui la versió estable de cada programari. • El seu objectiu principal la millora del programari. • D'una versió a la següent hi pot haver canvis significatius.. • És la release recomanada si es vol contribuir al projecte. • No es garanteix que el programari que conté el paquet funcioni correctament[72].

69 En aquest cas només contindran la informació del copyright i el fitxer changelog.Debian

70 No hi ha una correspondència directa paquet binari-paquet de fonts. Actualment a Debian hi ha uns 10000 paquets de fonts que generen entorn de 15000 paquets binaris.

71 N'hi ha d'altres de secundàries:

- amd64 -. contindrà els paquets per aquesta arquitectura mentre no se li doni suport oficial (http://www.debian.org/amd64). Mentre sigui així s'utilitza una clau diferent.
- experimental -. conté paquets no aptes per a l'ús públic. Destinat per a desenvolupadors
- volatile -. conté programari que hauria format part de l'stable si hagués existit en el seu moment, com pot ser escanejadors de virus, filtres d'spam o eines que han estat modificades (per exemple com a conseqüència d'una modificació de protocols).
- stable-proposed-updates i testing-proposed-updates- serveixen per “infringir deliveradament” les regles d'aquests archives. Tampoc se'n recomana l'ús públic.
- backports.org -. conté programari que originalment ha estat creat per a utilitzar llibreries posteriors a les que s'utilitzaven a l'stable que ha estat modificat i recompilat perquè utilitzi les antigues i així tenir disponible el programari a l'stable.

Estats del programari (official releases)	
	• No es garanteix que es compleixen les dependències entre paquets. • No es garanteix l'estabilitat del sistema.
testing	• Segon estadi dins del cicle de vida d'un paquet[73]. • Es busca un compromís entre les versions de cada paquet i l'estabilitat global del sistema. • El seu objectiu principal és la resolució d'errors de dependències cara la generació de la propera versió estable[74]. • És la release a utilitzar en la majoria dels casos.
stable	• Estadi final dins del cicle de vida d'un paquet. • L'objectiu fonamental és la consistència integral del sistema. • Només s'accepten actualitzacions per part del security team[75], i aquestes només poden millorar-ne la seguretat, i no poden aportar noves funcionalitats. • És la release a utilitzar en aquells sistemes en els quals l'estabilitat és fonamental, per exemple per a servidors de producció.

Codenames: unstable, testing, stable

Canonical names[76]: Sid[77], Etch[78], Sarge[79], etc.

72 En realitat, però, això succeeix molt poques vegades, ja que cal recordar que l'estabilitat del programari, en el sentit que aquest produeixi errors durant la seva execució, és un dels aspectes sobre el que es posa més èmfasis a l'hora d'acceptar un paquet dins de les releases oficials. A més a més, se suposa que el funcionament del programari en si mateix ja ha estat depurat dins del projecte particular que el produeix, i que quan s'inicia el seu procés de debianització, essencialment ja està lliure d'aquests tipus d'error. Els paquets que contenen programari potencialment inestable per ell mateix, versions de desenvolupament, s'acostumen a marcar con a *-snapshot (regla de facto).
Els errors més freqüents, per tant, dins d'aquesta release, són els de dependències entre paquets.

73 Cal tenir present que per raons de temporització dins del camí cap a l'estabilitat, les modificacions de seguretat dins de la testing poden tardar més dies que no pas per a la resta de releases.

74 El procés pel qual la release testing esdevé stable es coneix amb el nom de congelació. En aquest moment ja no s'accepta la incorporació de cap més millora en el programari i es centren els esforços en la resolució de conflictes de dependències. Un cop la testing congelada passa a stable l'estable anterior es passa a considerar obsoleta.
En aquest moment els administradors hauran de fer un apt-get dist-upgrade per a fer efectiu el canvi de release i resincronitzar-se amb els repositoris.

75 Grup que vetlla exclusivament per l'abolició de forats que podrien comprometre la seguretat del sistema.

76 tot i que, enteoria, el sistema apt ha d'impedir qualsevol dany, es recomana l'ús dels codenames a l'/etc/apt/sources.list per a referirse a les releases dels repositoris, ja que un canvi de release en els repositoris sense la corresponent adaptació del sistema local podria provocar forts conflictes de dependències.

77 La release unstable sempre rebrà el nom de Sid (el personatge dolent de les Toy Stories) ja que mai es congela.

78 És el nom amb què es designa la versió testing de la Debian 3.1.

79 És el nom amb què es designa la versió stable de la Debian 3.1.

Archives no oficials interessants	
apt-get.org[80]	Conté tot tipus de programari.
Christian Millart[81]	Programari multimèdia que no pot formar part dels oficials degut a incompatibilitats de les llicències amb les DFSG.

Estructura del Debian archive[82] (repositori[83])

/debian/[84] -> directori arrel[85]

/debian/dists/ -> índexs que associen les releases amb els paquets que les formen

/debian/pool/ -> tots els paquets

/debian/dists/canonicalname/release/binary-arch/Packages
/debian/dists/canonicalname/release/binary-arch/Packages.gz[86]
-> arxius (text pla, i text pla comprimit) que contenen tota la informació sobre els paquets de binaris que formen la secció[87] per una arquitectura

80 Web http://www.apt-get.org; és el primer lloc que cal consultar si un programari determinat no el trobem dins de les releases oficials.
81 Web http://debian.video.free.fr
82 Cal anar en compte perquè no tots els seus mirrors són complerts. En cas de dubte sempre es pot acudir als mirrors principals ftp.<codiDePaís(at,au,bg,...)>.debian.org. A http://www.debian.org/mirror/list hi ha la llista oficial d'aquests servidors, i una llista de servidors secundaris (els quals poden no ser complerts).
És navegable per web o ftp, per exemple a ftp://ftp.es.debian.org/debian/
83 Els repositoris de Debian estan en servidors accessibles via http o ftp. Constitueixen les fonts de descàrrega dels paquets.
84 Conté altres subdirectoris que tenen una rellevància menor:
- docs
- indices
- project
- tools -. eines per a la instal·lació (desfasades)

85 L'arrel de distribucions desfasades és /debian-archive/
86 Aquest és el fitxer que es va a buscar quan es fa un apt-get update. Si no hi és gzipped agafa el que no té compressió.
87 Per exemple /debian/dists/sarge/main/binari-i386/Packages:

```
Package: 3dchess
Priority: optional
Section: games
Installed-Size: 152
Maintainer: Stephen Stafford <bagpuss@debian.org>
Architecture: i386
Version: 0.8.1-11
Depends: libc6 (>= 2.3.2.ds1-4), xaw3dg (>= 1.5+E-1), xlibs (>> 4.1.0)
Filename: pool/main/3/3dchess/3dchess_0.8.1-11_i386.deb
Size: 33116
MD5sum: 7248665d99d529342a5cd050a9128ff6
Description: 3D chess for X11
 3 dimensional Chess game for X11R6.  There are three boards, stacked
 vertically; 96 pieces of which most are the traditional chess pieces with
 just a couple of additions; 26 possible directions in which to move.  The
```

/debian/dists/canonicalname/release/binary-arch/Release
-> arxiu (text pla) d'informació sobre secció i l'arquitectura[88]

/debian/dists/canonicalname/release/source
-> directori a on hi ha la informació per trobar els paquets de fonts

/debian/pool/release/{[0-9],[a-z],lib-,lib[0-9],lib[a-z]}/packagename/
-> directoris a on hi ha els continguts dels paquets (binaris i fonts) i informació sobre aquests:

binaris:
packagename_debversion[89]_arch.deb[90]
-> conté els binaris, llibreries, documentació, etc. de la versió debversion del paquet package per a l'arquitectura arch:

debian-binary -> un “magic” per a identificar l'arxiu com a paquet de Debian. Es correspon a la versió del format de paquet (actualment la 2.0)

control.tar.gz -> tarball que conté informació per a les eines d'administració de paquets. S'hi poden trobar els arxius de configuració i scripts següents:

conffiles	Tots aquests fitxers (en referència absoluta) rebran un tractament especial per a conservar les modificacions fetes per l'usuari en versions anteriors[91].
config	Script que serveix per a obtenir la informació de

```
 AI isn't wonderful, but provides a challenging enough game to all but the
 most highly skilled players.

Package: 3ddesktop
Priority: optional
Section: utils
Installed-Size: 360
Maintainer: Mathias Weyland <mathias@weyland.ch>
Architecture: i386
Version: 0.2.8-1
...
```

88 Per exemple /debian/dists/sarge/main/binary-386/Release

```
Archive: stable
Version: 3.1r1
Component: main
Origin: Debian
Label: Debian
Architecture: i386
```

89 Versió dins de Debian: versióDinsDelProjecteOriginalDeDesenvolupament(X.Y.Z)-versióEnElProcésDeDebianització(A.B)

90 Mitjançant el preprocessador lesspipe la comanda less pot mostar les dades més importants d'un fitxer .deb:
$ export LESSOPEN=”|lesspipe %s”
$ less fitxer.deb

91 Així es garanteix que una actualització no impliqui la pèrdua de la configuració del programari.

	l'usuari necessària per a la configuració del paquet[92].
control	Metainformació sobre el paquet i la verificació de dependències prèvies a la instal·lació[93].
md5sum	Sumatori MD5 del contingut del paquet[94].
postinst	Script que s'executa com a part del procés d'instal·lació un cop s'ha finalitzat el desempacatat. S'executarà tot i que el procés d'instal·lació o upgrade falli.
postrm	Script que s'executa després que el paquet s'hagi tret del sistema. dpkg fa saber si s'ha desinstal·lat o purgat perquè actuï en conseqüència.
preinst	Script que s'executa abans de la instal·lació o upgrade d'un paquet. Si l'upgrade d'un paquet falla es proba d'executar el preinst de la versió anterior perquè provi de desfer els possibles canvis deguts al procés d'upgrade fallit.
prerm	Script que s'executa abans de la retirada del paquet del sistema. Si es fa un upgrade, s'executarà el prerm de la versió anterior.
shlibs	Llistat de les llibreries[95] que aporta el paquet al sistema. Durant el procés d'establiment de dependències es fan servir tots els shlibs de tots els paquets per determinar quines llibreries aporta finalment cada paquet i en quines versions.
templates	

data.tar.gz -> tarball que conté tot el programari tal i com quedaria instal·lat si el desempaquetéssim a l'arrel del sistema (/)

`packagename_debversion_arch`.diff.gz ->

`packagename_debversion_arch`.dsc ->

92 La informació que introdueix l'usuari queda emmagatzemada a la cache del debconf cara al seu processat posterior per la resta d'scripts (postinst, per exmple).
93 Aquest és l'únic fitxer de control que ha de contenir el control.tar.gz obligatòriament.
94 Permet, utilitzant els mecanismes pertinents, garantir la integritat del paquet; entre d'altres, serveix per a detectar-ne alteracions malicioses.
95 i dels SONAMEs (noms pels quals el linkador dinàmic identifica les llibreries i els binaris que els corresponen).

fonts[96]:

`packagename_debversion`.dsc -> Informació essencial per a la descripció dels altres dos paquets de fonts; n'inclous els seus sumatoris MD5, així com la signatura del mantenidor i autentifica el procés d'upload a l'archive.

`packagename_version`[97].orig.tar.gz -> Codi font tal i com s'ha obtingut del projecte original a on es desenvolupa el programari

`packagename_debversion`.diff.gz -> Codi afegit al codi font original durant el procés de debianitzacio[98]

Classificació dels paquets

Prioritat dels paquets	
required	Paquets necessaris per a garantir el funcionament correcte del sistema. No s'han d'esborrar mai si no es vol comprometre la integritat del sistema. Sense aquests paquets el sistema és inutilitzable tot i que si que arranca per permetre la instal·lació de més paquets
important	Paquets que proporcionen les funcionalitats que té qualsevol sistema UNIX-like.
standard	Programari que estén, raonablement, la funcionalitat del sistema. La instal·lació mínima[99] de Debian es nodreix exclusivament d'aquest grup i els dos anteriors.
optional	Programari que, raonablement, instal·larem per a treballar amb el sistema. Aquí hi trobem conjunts de programari com les X o TeX. Aquests paquets no haurien de generar conflictes amb cap dels

96 Si l'operació essencial que es fa amb els paquets binaris és la descàrrega per a la seva instal·lació, l'operació fonamental amb els paquets de fonts és la seva càrrega al repositori principal, ja que és allà a on, un cop finalitzat el procés de càrrega dels paquet de fonts, es realitza el procés de compilació per a l'obtenció dels paquets binaris. Un cop finalitzat el procés de creació dels binaris comença el procés de propagació d'aquests cap a tots els repositoris oficials.

97 Versió dins del projecte original de desenvolupament del programari, X.Y.Z. No s'ha de confondre amb la debversion que és la versió que té el programari dins de Debian un cop ha estat debianitzat; aquesta la formen les tres ternes anteriors-A.B

98 El codi complet resultant de la debianització s'obté patchajant el codi font original amb les aportacions de debian.

99 El sistema mínim de Debian conté per defecte 123 paquets i ocupa 97Mb un cop acabada la instal·lació.
De fet, però, aquest sistema mínim encara se li podrien treure els paquets que es llisten a continuació i al sistema resultant encara se li podria dir UNIX-like: dash, dhcp-client, exim4, exim4-base, exim4-config, exim4-daemon-light, info, initrd-tools, ipchains, iptables, libgcrypt1, libgnutls7, libident, liblockfile1, liblzo1, libnewt0.51, libopencdk8, libcap0.7, libpcre3, libsigc++-1.2-5c102, libssl0.9.7, libtasn1-0, libtextwrap1, locales, mailx, makedev, nano, pcmcia-cs, ppp, pppconfig, pppoe, pppoeconf, setserial, tasksel, telent, wget.

Prioritat dels paquets	
	pertinents a grups anteriors.
extra	Hi ha tots els paquets que generen conflictes amb pertinents a la resta de grups. Només té sentit instal·lar-los si sabem exactament perquè els necessitem.

Categories dels paquets[100]	
Section name	**Descripció**
admin	Utilitats d'administració del sistema
base	Sistema base de Debian
comm	Programari per a dispositius de comunicació
devel	Utilitats i programes per al desenvolupament de programari
doc	Documentació i tot el programari especialitzat per a la seva visionat
editors	Editors i processadors de textos
electronics	Programari per a treballar amb circuits
embedded	Programari per a sistemes encastats
games	Jocs i d'altres divertiments
gnome	Programari de l'entorn d'escriptori GNOME
graphics	Utilitats per a la creació, visionat i edició de fitxers gràfics
hamradio	Programari per als radioaficionats
interpreters	Intèrprets per als llenguatges interpretats
kde	Programari de l'entorn d'escriptori KDE
libdev	Arxius de desenvolupament de llibreries
libs	Reculls de rutines de programari
mail	Programari per a la redacció, emissió i enrutament de correu electrònic
math	Programari per a l'anàlisi numèric
misc	Programari de miscel·lània
net	Programari per a la connexió en xarxa
news	Clients i servidors de Usenet
oldlibs	Llibreries obsoletes
othersfs	Emuladors i programari per a sistemes de fitxers foranis
perl	Llibreries i intèrprets de Perl
python	Llibreries i intèrprets de Python

100Segons la Debian policy.

Categories dels paquets	
science	Programari per al treball científic
shells	Comandes de consola i entorns de consola alternatius
sound	Utilitats per a l'edició i reproducció de so
tex	El sistema d'edició de text TeX
text	Utilitats de processament de text
utils	Diverses utilitats de sistema
web	Navegadors de Web, servidors, proxies i d'altres eines
x11	L'X Window System

Autenticitat dels paquets dels repositoris

- Els paquets oficials estan convenientment signats.
- A partir de l'Etch durant la seva instal·lació es comprova l'autenticitat de les claus[101].
- El paquet debian-keyring conté les claus dels desenvolupadors.

BTS Bug Tracking System

- És el mecanisme per a la posada en coneixement als desenvolupadors de l'existència de bugs.
- Cal seguir les normes estàndard per aquest tipus de missatges:
  - Un sol bug per missatge
  - Plataforma
  - Distribució
  - Kernel / mòduls / llibreries
  - Aportar la màxima informació possible de com s'ha trobat i exposar si es pot reproduir per a ser estudiat
- Per al primer bug, abans d'omplir el formulari de notificació és recomanable llegir-ne uns quants per veure'n alguns exemples.
- Cal ser conscients que davant d'un bug cal notificar-ho sempre[102], ja que és una de les manera de contribuir a la millora dels projectes.
- Paquet per a la obrir/seguir de bus: reportbug.

101 Més informació al Securing Debian Manual http://www.debian.org/doc/manuals/securing-debian-howto/.

102 Comprovant, abans de fer-ho, que no existeixi ja la notificació de la seva trobada.

- Web http://www.debian.org/Bugs

Instal·lació[103] de GNU/Linux Debian Etch[104]

Tipus d'instal·lació de Debian	
full	A partir dels Cds/DVDs oficials (http://www.debian.org/CD/) • Contenen tots els paquets que integren la distribució[105] Es poden obtenir: • comprant-los/copiant-los • descarregant-los per xarxa: • jido: http://www.debian.org/CD/jigdo-cd/ • És el mètode recomanat des de Debian • BitTorrent: http://www.debian.org/CD/torrent-cd/ • Usa la tecnologia peer to peer • .iso[106]: http://www.debian.org/CD/http-ftp/ • Es demana evitar l'ús d'aquest mètode
netinst[107]	Imatge preparada per gravar-la en un CD: • Conté tot el necessari per a instal·lar i configurar el sistema Debian estàndard. • La resta del programari s'obté per xarxa d'algun dels repositoris de Debian. • De 100 a 150Mb segons les plataforma. • Diàriament es fan imatges[108] a: http://cdimage.debian.org/cdimage/daily-builds/daily/arch-latest/
business card[109]	Imatge pensada per cabre en un CD mini: • Funciona com el netinst, però no incorpora el sistema bàsic, el qual s'obté per xarxa.
netboot	Permet, amb el maquinari adequat, utilitzant PXE i Bootp, fer la instal·lació per xarxa sense necessitat ni de CDs ni diskets.

103 Els sistemes UNIX es caracteritzen per ser molt robustos, i rarament cal que, un cop feta una instal·lació, aquesta s'hagi de repetir (reinstal·lar) al cap d'un temps perquè alguna cosa ha deixat de funcionar. Cal tenir present que quasi bé tot el que integra el sistema es pot modificar des del mateix sistema, i que, encara que es produís una catàstrofe, sempre se'n poden reaprofitar moltes parts. En aquest aspecte, segurament el més crític és la corrupció física dels discs durs; una bona política de backups pot estalviar molts mal de caps.

104 La instal·lació Sarge és pràcticament igual. Per a la instal·lació de Sid, tot i que hi ha la possibilitat de instal·lar-la directament (no oficial), primer cal instal·lar Sarge (o Etch) i després fer un dist-upgrade.

105 Normalment, però, amb els tres o quatre primers CDs o amb el primer DVD n'hi ha prou per obtenir un sistema plenament operatiu.

106 Hi ha clients (navegadors) que per motius de seguretat per defecte no permeten la descàrrega d'arxius tan grans.

107 Constitueix la instal·lació més còmode si es disposa d'un ample de banda raonable (amb una connexió ADSL de 512kb/s funciona acceptablement bé)

108 Cal tenir present, però, que són testing i que ocasionalment podrien fallar.

109 De moment només es suporten les connexions Ethernet.

Tipus d'instal·lació de Debian	
hd-media	Per a fer la instal·lacion, amb el maquinari adequat[110], des d'un dispositiu de magatzematge USB.
floppy[111]	Permet fer la instal·lació des de disquets: • Funciona com el bussinesscard.

L'installer[112] de Debian

És el programa encarregat de gestionar la instal·lació de Debian. Les seves característiques principals són:

- Modular:
  - En facilita la particularització.
  - El fa pràcticament independent de l'arquitectura.
- Molt potent pel que fa a la detecció de maquinari (hw-detect i discover):
  - Pesat per explotar les innovacions en aquest camp dels kernels 2.6[113]
- Modes estàndard i expert per a regular el nivell d'interacció amb l'administrador
- Possibilitat de pas de paràmetres a l'arrancada per a maquinari “extrany”
- Particionament millorat:
  - Es poden crear RAIDs i LVMs abans de procedir al particionament
  - Es poden copiar, moure i modificar la grandària de les particions[114]
- De manteniment relativament senzill a nivell de codi i concebut per a facilitar possibles ampliacions futures.
- Internacionalització (el procés es pot seguir en més de 50 llengues diferents)

110bàsicament cal que la placa mare ha de permetre l'arranc des de dispositius USB.
111També existeix l'opció access-floppy pensada per a usuaris invidents.
112Per a Sarge s'ha reescrit des de zero; aquesta ha estat una de les raons principals que han fet que hi hagi un espai de temps important entre aquesta release i la anterior (Woody).
113Tot i que també pot utilitzar els kernels 2.4.
114Per a la majoria de filesystems soportats.

- S'integra totalment el suport Wireless que ofereixen els kernels 2.6[115]

-> Es especialment interessant cara a instal·lacions massives (clústers, oficines, etc.)

-> Utilitzant eines com fai i cfengine es poden aconseguir instal·lacions totalment automatitzades sense necessitat de cap interacció.

Nota: per fer el seguiment de la instal·lació vegeu el contingut de installacióDebian.odp.

Apt

L'ús de dpkg no és recomanable[116] ja que està fora dels estàndards actuals de l'administració de paquets[117] => és bo acostumar-se a l'ús d'apt[118].

L'apt és una llibreria que facilita el manegament de paquets. L'administrador l'utilitza bàsicament amb dos front-ends: apt-get[119] i apt-cache[120]

Especificació de repositoris		
Fitxer		
/etc/apt/sources.list[121]		
Sintaxi		
tipus uri distribució [component1] [component2] [...]		
Valors		
tipus	deb	Per a repositoris de binaris
	deb-src	Per a repositoris de fonts

115 Desafortunada ment a hores d'ara el suport d'aquests dispositius per part de la línia central del kernel és més aviat escàs degut a la disparitat de projectes que hi ha en aquest terreny.
116 Tot i això la consistència de Debian la garanteix la robustesa de dpkg.
117 Per exemple careix de resolució automàtica de dependencies.
118 És una eina d'alt nivell que s'ha desenvolupat per cobrir les deficiències de dpkg.
119 És necessita tenir permisos de root per a la seva execució.
120 La seva execució ne requereix permisos especials.
121 Després de l'edició del fitxer sempre cal fer un apt-get update per actualitzar la base de dades i poder accedir així als nous recursos.
Aquest fitxer també es pot modificar de manera assistida amb apt-setup.
El fitxer es pot generar de forma automàtica en base a l'accessibilitat dels repositoris amb apt-spy.

Especificació de repositoris		
uri	cdrom[122]	Per afegir CDROM s'ha d'utilitzar apt-cdrom[123]
	file	Permet l'ús d'un filesystem local com a repositori
	copy	Com file però utilitza el directori cache[124] per emmagatzemar els paquets baixats
	http	p. ex. http://http.us.debian.org/debian
	ftp	p. ex. ftp://ftp.es.debian.es/debian
	ssh	Connexió SSH que no necessita passwd.
distribució[125]	sarge	
	etch	
	sid	
components	main	
	dist	
	Non-free	

Exemple d'/etc/apt/sources.list:

```
deb http://ftp.es.debian.org/debian/ etch main
deb-src http://ftp.es.debian.org/debian/ etch main

deb http://security.debian.org/ etch/updates main
deb-src http://security.debian.org/ etch/updates main
```

Paquests de diferents releases

És possible instal·lar programari de diferents releases. Per això cal crear el fitxer /etc/apt/preferences a on s'establiran les preferències a l'hora d'extreure paquets de les releases. Exemple d'/etc/apt/preferences:

- exemple:

```
Package:*
Pin: release a=testing
Pin-Priority[126]: 900

Package: *
```

122Amb aquest mètode no es cachegen els paquets.
123apt-cdrom –cdrom /media/cdrom utilitzarà /media/cdrom com a mount point.
124/var/cache/apt/archives/
125Com ja s'ha argumentat, és preferible l'ús dels condenames que els noms canònics.
126Pin-Priority:
P <= 0 els paquets amb prioritats negatives no s'instal·laran mai.
0 < P <= 100 els paquets s'instal·len només si no n'hi ha una versió prèvia instal·lada.
100 < p <= 1000 els paquets s'instal·len de forma automàtica si no hi ha una versió anterior instal·lada amb prioritat superior. No hi haurà mai downgrades.
1000 < P els paquets s'instal·len o s'upgradeigen de forma automàtica tot i que n'hi hagi una versió prèvia instal·lada amb prioritat superior.

```
Pin: release a=unstable
Pin-Priority: 90
```

Instal·lació de paquets[127]
apt-get install `llistaDePaquetsAInstallar`

Tots els paquets instal·lats es cachegen a /var/cache/apt/archives/

Resolució de dependències
El mateix apt-get install proposa la instal·lació dels paquets necessaris per satisfer totes les dependències[128].

Reinstal·lació de paquets
apt-get install --reinstall `llistaDePaquetsAReinstallar`

Consultes a la base de dades d'apt[129]	
apt-cache search `patró [patró2]`	Es busquen els paquets que contenen patró. Hi ha d'haver tots els patrons especificats
apt-cache show `nomPaquet`	Mostra la informació sobre el paquet
apt-cache showpkg `nomPaquet`	Mostra més informació[130] sobre el paquet

Actualització de la base de dades	
apt-get update	Convé fer-ho regularment[131]

Actualització del sistema	
apt-get upgrade	Fa que tots els paquets instal·lats

127 No s'ha d'instal·lar més programari d'aquell que és estrictament necessari per donar resposta a unes necessitats determinades.
Alguns dels perjudicis de la instal·lació de programari innecessari són:
- Disminució del rendiment del sistema
- Incorporació potencial de vulnerabilitats; cal ser especialment prudent amb els servidors
- Més programari a actualitzar

128 Si un paquet depèn d'un tercer paquet o d'un quart paquet, apt instal·larà el tercer paquet, el primer que troba, i no el quart perquè ja queden satisfetes les dependències. Si es vol que s'instal·li el quart en comptes del tercer, s'ha d'especificar al apt-get isntall llistaDePaquets.

129 També és de molta utilitat a l'hora de buscar paquets http://packages.debian.org

130 Com les dependències reverses.

131 És pot utilitzar el sistema cron-apt per automatizar aquesta i d'altres tasques.

Actualització del sistema	
	s'actualitzin a l'última versió disponible[132].

Upgrade de distribució[133]	
apt-get dist-upgrade	

Desinstal·lació i eliminació de paquets[134]	
apt-get remove `nomPaquet`	Desinstal·la (coservant els arxus de conf).
apt-get remove --purge `nomPaquet`	Elimina (eliminant tots els arxius).

Eliminació dels paquets del cache[135]	
apt-get autoclean	Elimina els paquets desfasats.
apt-get clean	Elimina tots els paquets.

Altres	
apt-get --fix-broken install	Reprèn les instal·lacions i/o configuracions que hagin pogut quedar interrumpudes.
apt-get install --download-only paquet	Només es baixa el .deb; no s'instal·la.
--simulate	Sempre es pot afegir aquesta opció per veure “què passaria si...”

apt-file[136]	
apt-file update	Per crear la base de dades, que és independent de la d'apt
apt-file list `nomPaquet`[137]	Llista tots els fitxers que pertanyen al paquet

132Convé sempre abans fer un apt-get update per tenir actualitzada la base de dades local. També pot ser convenient automatitzar aquesta tasca.

133Abans d'executar l'apt-get dist-upgrade cal especificar la nova release a /etc/apt/sources.list i fer un apt-get update.

134No és el mateix: quan un paquet es desinstal·la els arxius de configuració queden al sistema cara a una futura instal·lació. Si s'eliminen es perden tots els fitxers que ha aportat el paquet al sistema.

135/var/cache/apt/archives/.

136apt-file no forma part de la instal·lació bàsica. Cal instal·lar el paquet apt-file i fer un apt-file update immediatament per a crear la base de dades i poder utilitzar apt-file.

137Per llistar els continguts d'un paquet no cal que estigui instal·lat (d'aquí la necessitat de crear una base de dades independent).

Altres aplicacions per a la gestió de paquets	
dpkg	És l'espina dorsal del sistema de paquets de Debian.
dpkg-reconfigure	Seguit del nom d'un paquet instal·lat, serveix per tonar a presentar les opcions de configuració d'instal·lació.
dselect	Interfície de text. Molt potent. El seu ús no és trivial. És força utilitzat per raons històriques.
tasksel	Interfície de text molt simple. Només permet la instal·lació de grans conjunts de paquets.
aptitude	Pot treballar en mode comanda[138] o en mode interfície basada en ncurses.
synaptic	Interfície gràfica X. És una alternativa a aptitude.
wajig	Front-end simplicat.
deborphan	Identifica els paquets que han quedat orfes i que no els utilitza cap altre paquet[139].
debfoster	Identifica aplicacions amb finalitzats similars.

Creació de paquets .deb

- http://www.tldp.org/HOWTO/html_single/Debian-Binary-Package-Building-HOWTO/
- http://www.debian-administration.org/articles/336
- http://people.warp.es/~isaac/debian-packaging-tutorial-es.pdf

Les X i aplicacions

Paquet / Metapaquet principals	Contingut
x-window-system-core	Servidor X Una sel·lecció bàsica de fonts Llibreries gràfiques fonamentals Les utilitats X més bàsiques[140]

138En mode comanda accepta quasi bé tots els paràmetres de apt-get, tot i que de vegades tenen comportaments lleugerament diferents davant dels mateixos paràmetres. Si apt-get falla en algun moment, aptitude amb els mateixos paràmetres pot ser una bona alternativa.
139Deborphan | xargs dpkg --purge
140Entre les que no hi ha un emulador de terminal.

Paquet / Metapaquet principals	Contingut
x-window-system	Tot l'x-window-system-core més: Servidor de fonts Servidor d'impressió X twm xterm
gnome-core	Nucli del desktop manager
gnome-desktop-environment	El que és habitual en un GNOME
openoffice.org-core	Nucli de la Suite Openoffice.org
openoffice.org[141] `$ make install`[142]	El que és habitual a l'Openoffice.org
mozilla	Suite Mozilla
mozilla-firefox	Firefox
mozilla-thunderbird	Thunderbird
tetex-base	Infrastructura per a TeX

Particularitats de Debian

L'ús de directoris en comptes de fitxers per a la configuració

- Tècnica introduïda per Debian per facilitar l'administració i l'accés a fitxers de configuració per part del sistema de paquets.
- Consisteix en ampliar les capacitats de configuració que ofereix un fitxer en altres fitxers que resideixen en subdirectoris d'/etc/ i que l'aplicació configurada els llegeix com si formessin part del fitxer de configuració.
- Exemple: cron; /etc/crontab s'expandeix a /etc/cron.d/

El sistema d'alternatives

- Serveix per:
  - Evitar la instal·lació d'aplicacions que tenen una mateixa finalitat degut a dependències.
  - Per facilitar la selecció d'aplicacions instal·lades que tenen la mateixa finalitat.

141 El sistema de correcció ortogràfica està integrat en myspell. Per tant, per afegir el corrector ortogràfic català només cal fer un apt-get install myspell-ca i reiniciar l'OOo.

142 Habitualment requerirà permisos de root.

- Exemple: els editors de text
- Estratègia:
    - Els paquets que necessiten un editor de text no especifiquen un editor en concret, sinó que alerten, durant el procés d'anàlisis de dependències, que el sistema ha de tenir un editor instal·lat.
    - En el sistema, durant el procés d'instal·lació del primer editor es crea el fitxer /usr/bin/editor, un symlink que apunta a /etc/alternatives/editor, el qual al mateix temps és un altre symlink que apunta al binari que es vol utilitzar com a editor per defecte.
- S'administren mitjançant la comanda update-alternatives
    - Dues maneres d'establir-les:
        - manual: el sistema sempre les respectarà el que hagi establert l'administrador. Exemple:
          ```
          update-alternatives --set editor /bin/ed
          ```
        - auto: un sistema de prioritats establirà en cada moment quina és l'aplicació que s'utilitzarà. Exemple:
          ```
          update-alternatives --auto editor
          update-alternatives --display editor
          ```

Usuaris i grups

UID i GID	
Rang ID	***proposit***
0-99	IDs estàtics preestablerts. Presents a quasi bé tots els sistemes Debian
100-999	IDs creats dinàmicament durant la instal·lació de paquets per a comptes de sistema.
1000-29999	IDs per a usuaris estàndard creats per adduser i addgroup
30000-59999	Reservats per a l'ús local per l'administrador
60000-65533	IDs estàtiques preestablerts utilitzats si hi ha petició
65534	Usuari nobody
65535	No es pot utilitzar

Comptes de sistema	
nom	**finalitat**
root	Superusuari. Estàndard UNIX.
sync	Pensat exclusivament per a fer front als atacs per denegació

Comptes de sistema	
	de servei. Força la sincronia dels discs.
www-data	Normalment els servidors en Debian corren sota aquest usuari. Els fitxers que contenen les dades que serveixen no haurien de pertànyer a aquest usuari per raons de seguretat[143].
nobody	Els daemons que no són propietaris de fitxers poden córrer sota aquest usuari, tot i que es recomana que sempre tinguin el seu propi usuari.

Els scripts d'/etc/init.d/

- Serveixen per manegar els serveis
- Com a mínim han de permetre:
  - start -> engega el servei
  - stop -> atura el servei
  - restart -> atura i torna a engegar el servei
  - reload -> força la relectura de la configuració del servei sense reiniciar-lo
  - force-reload -> assegura la relectura de la configuració mitjançant reload o si falla amb restart
- Els fitxers de configuració d'aquests scripts[144] estan a /etc/default/
- L'aplicació start-stop-daemon facilita la creació dels scripts
- Els symlinks als scripts de serveis que s'executaran durant l'engegada o canvi de runlevel estan a /etc/rcN.d/ a on N és el runlevel. La seva nomenclatura estableix en l'ordre que s'aniran executant els diferents scripts i és la següent:

  [K|S] + nn + [cadena]

  - La primera lletra serà S si el servei s'ha d'engegar, o K si s'ha d'auturar.
  - El segon i el tercer caracter formaran un numero de dos digits:
  - La cadena s'acostuma a fer coincidir amb el nom de l'script de /etc/init.d/
- Els symlinks d'/etc/rcS.d/ es seguiran sempre

143Tot i que hi pot haver aplicacions que així ho requereixen de web; mal dissenyades.
144No dels serveis.

- La comanda update-rc.d serveix per gestionar aquests symlinks[145]
- La comanda invoke-rc.d serveix per a cridar els scripts de /etc/init.d/[146]

Runlevels[147]	
0	Halt; aturada del sistema
1/S	Single user mode; estableix els scripts mínims en qualsevol engegada del sistema
2	Estàndard, mode multiusuari
3,4,5	No estan definits
6	Reboot; reinici.

145També es pot fer manualment amb `ln -s`.
146Tot i que a la pràctica es solen invocar directament pel seu nom.
147És específic de Debian.

3r Capítol: Usuari

Conceptes provinents del kernel

Inode

- Conté un número unívoc que identifica un fitxer.
- N'hi ha un per a cada fitxer del sistema.
- A més a més conté:
    - Un comptador que compta els hard links que hi ha sobre el fitxer i les vegades que el sistema el té obert[148].
    - UID del propietari.
    - GUID del grup.
    - Els permisos del fitxer.
    - La longitud del fitxer en bytes.
    - Les adreces dels blocs de dades[149].
    - La informació de l'últim cop que s'ha modificat el fitxer.
    - La informació de l'últim cop que s'hi ha excedit.
    - La informació de l'últim cop que s'ha modificat l'inode.

Tipus de fitxers

- Constituents dels filesystems de UNIX
    - Fitxers regulars
    - Directoris
    - Links simòlics[150]
- Fitxers de dispositius relacionats amb E/S (device files o drivers)
    - Orientats a blocs
    - Orinetats a caràcters
- Comunicacions entre processos
    - Pipes
    - Semàfors
    - Memòria compartida

148La comanda lsof llista els fitxers oberts.
149O major and minor device numbers.
150Coneguts com a symlinks.

- major and minor device numbers

Fitxers regulars

- Són ternes de:
  - Parella nom_de_fitxer – #inode
  - Inode
  - Stream de dades

Directoris

- Taula de parelles nom_de_fitxer – #inode

Enllaços[151]

- Enllaços durs[152]
  - Només hi ha un inode i un stream de dades
    - a awuest inode hi fa referències més d'una parella nom_de_fitxer – #inode
  - Segur que existeix el contingut
  - Només es poden fer dins del mateix filesystem

- Enllaços febles
  - Només hi ha un stream de dades
  - hi ha un inode per a cada parella nom_de_fitxer – #inode
    - només el primer inode té les adreces als blocs de dades
    - a la resta d'inodes el path a dades fa referència a la parella nom_del_primer_fitxer – #inode
  - Pot ser que apuntin a fitxers inexistents

151A http://linuxgazette.net/105/picther.html es pot trobar una explicació entenedora dels fonaments d'ambdós tipus d'enllaços.
152Tenen el mateix número d'inode; cosa que es pot comprovar amb el paràmetre -i de la comanda ls.

- passa quan s'esborra el primer fitxer generat, ja que en el seu inode no hi ha informació sobre el fet que altres parelles nom_de_fitxer – #inode el necessiten

Entrades i sortides

- A UNIX tot el que accepta o produeix dades és un fitxer[153].
  - L'única manera d'acceptar dades és per l'*standard input (STDIN)*.
  - L'única manera de produir dades és per l'*standard output (STDOUT)*.
  - L'única manera de produir missatges d'error és per l'*standard error (STDERR)*.

SUID, SGID

- “s” en comptes d'“x” a propietari i/o a grup.
- El programa s'executarà com si l'hagués llençat el propietari[154]

Sticky bitk

- “t” en comptes d'“x” a altres en directoris
- Dins del directori només podrà eliminar i canviar de nom els fitxers el propietari.
- Útil en directoris d'accés públic.

La shell

- La seva tasca és la de traduir les línies de comandes d'usuari a instruccions de sistema operatiu.
  => és un macro processador que executa comandes.
  - Per exemple: `sort –n llista.txt > llista.ordenada.txt`

    A grans trets[155] implica:

    1. Trenca la línia en *paraules*:

153Inclòs el maquinari.
154Per exemple, cada cop que s'executi /usr/bin/login (-r-sr-xr-x 1 root wheel) s'executarà amb permisos de root, independentment de que l'hagi invocat.
155Òbviament cada un d'aquests passos realment implica molts subpassos, cadascun dels quals inclou una instrucció particular del sistema operatiu que hi ha per sota.

```
sort
-n
llista.txt
>
llista.ordenada.txt
```

2. Determina la finalitat de cada paraula:

```
sort                    -> és una comanada
-n                      -> és un argument de sort
llista.txt              -> és un argument de sort
> llista.ordenada.txt   -> juntes són instruccions I/O
```

3. Configura les I/O[156] d'acord amb `> llista.ordenada.txt`

4. Troba la comanda sort a un fitxer i l'executa amb l'opció -n (ordre numèric[157]) i l'argument llista.txt (fitxer d'entrada).

- La shell en sí no és UNIX, sinó que tan sols és una interfície per aquest, ja que UNIX és un "user interficie independent SO[158]".

- Permet l'execució de comandes de forma:

  - síncrona => no es pot executar una altra comanda fins que l'anterior no ha acabat.

  - Asíncrona => la shell no espera que la comanda que s'està executant hagi acabat per acceptar noves comandes (background).

- Es pot utilitzar:

  - interactivament => les entrades es fan per teclat. Just després de loginejar-se ja s'hi entra. En bash, per sortir-ne `exit`, `logout` o Ctrl-D[159].

  - no-interactivament => les entrades s'agafen d'un fitxer.

- Com qualsevol altre llenguatge de programació d'alt nivell, proporciona:

  - variables
  - estructures de control de flux
  - quoting[160]
  - funcions

- A nivell interactiu, permeten:

156 I també fa algunes altres operacions estàndard implícites.
157 `man sort`
158 Això s'ha traduït en l'aparició de diverses shells, cadascuna amb les seves particularitats.
159 De fet, però, és recomanable desactivar aquesta tecla de control perquè és més possible que es premi per error que no pas amb la intenció de sortir realment del bash.
160 Literals; per evitar-ne la seva interpretació com a comandes.

    - control de tasques.
    - edició de la línia de comandes.
    - històrics.
    - aliases.

- Built-in commands (*builtins*): comandes que aporta el propi shell

    - impossibles d'implementar externament[161]. Per bash: `cd`, `echo`, `continue`, `exec`, `type`, etc.
    - o que no convé la seva implementació externa. Per bash: `kill`, `pwd`, `getopts`, `history`, etc.

Bash[162]

- Desenvolupat per GNU => GPL

- És la shell per defecte de molts sistemes UNIX i també s'ha portat a d'altres SO.

- Bash reference manual: http://www.gnu.org/software/bash/manual/bash.html

Nom de fitxers, comodins, i expansió de rutes

Comodí	Correspondència
?	Qualsevol caràcter sol
*	Qualsevol cadena de caràcters
[conjunt]	Qualsevol caràcter del conjunt
[!conjunt]	Qualsevol caràcter fora del conjunt

Expressió	Correspondència
[abc]	a, b, o c
[.,;]	Punt, coma o punt i coma
[-_]	Guió o guió baix
[a-c]	a, b, o c
[a-z]	Totes les lletres minúscules
[!0-9]	Tot els no-nombres

161 En un fitxer executable, com passa amb la majoria de comandes: `ls`, `sort`, `cat`, `ps`, etc.

162 Acrònim de Bourne-Again shell, nascut oficialment al 10 de gener de 1988, és successor del Burne shell (conegut com sh), inclou les característiques més interessants del C shell i del Korn shell.

Expressió	Correspondència
[a-zA-Z]	Totes les minúscules i les majúscules

Expressió	*Exemples*
b{ar{d,n,k}ed}	Bards, barns, barks, beds

Descriptors de fitxers

- Tot fitxer obert té associat un descriptor

Descriptor	Fitxer
0	STDIN
1	STDOUT
2	STDERR
3...9[163]	Per a la resta de fitxers oberts

Redirectors

- Els redirectors permeten redirigir entrades i sortides a d'altres fitxers.
  - Entrada estàndard: `comanda < nomdefitxer`
  - Sortida estàndard: `comanda > nomdefitxer`
    `comanda >> nom de fitxer`[164]

    Per exemple: `cat <fitxerorigen >fitxerdestí`[165]

    -> agafa el contingut de `fitxerorigen` i l'escriu a `fitxerdestí`[166]

  - Sortida de missatges d'error: `2> nomdefitxer`
  - STDOUT i STDERR juntes: `&> nomdefitxer`
  - STDERR cap a STDOUT: `2>&1`

163De vegades és l'associar els descriptors fitxers estàndards a algun dels descriptors sobrants(i>&j) per estalviar-se l'haver de desfer canvis posteriorment per restaurar les condicions inicials.

164Mentre >> fa que el contingut de la sortida estàndard s'afageixi als continguts, si existeixen, de `fitxerdestí`, > sobreescriu a sobre els possibles continguts de `fitxerdestí`, i per tan al final aquest només contindrà els resultats de la sortida estàndar de l'última comanda que s'ha redireccionat sobre el fitxer.

165Aquesta línia por servir de substitut a la comada cp, ja que el resultat serà dos fitxers amb nom diferent però amb continguts iguals.

166Estrictament, cat el que fa és escriure a la sortida estàndard el que hi ha a l'entrada estàndard. En aquest cas, però, ambdues s'han redireccionat sobre fitxers. Opcionalement també accepta noms de fitxers com a paràmetre d'entrada per a escriure el seu contingut per a la sortida estànard

- Les pipelines permenten redirigir directament la sortida d'una comanda a l'entrada de la comanda que la succeeixi.

  -> els filtres permeten anar refinant els continguts del text d'entrada.

  -> filtre i patró són conceptes indissociables.

  Per exemple: `cut -d: -f1  < /etc/passwd | sort`

  -> fa que la sortida de la comanda cut[167], que és la primera columna[168] del fitxer passwd vagi a l'entrada de la comanda sort. Per tant la línia retornarà una columna de tots els usuaris del sistema ordenada per ordre alfabètic.

Patrons i expressions regulars[169]

- Les expressions són instruccions de com fer coincidir patrons.
- Fer coincidir patrons s'aconsegueix emprant text i tokens especials.
- Exemples:
  - l'expressió `root` coincideix amb `root:x:passworDencriptat:10717:0:99999:7:::` però no amb `Enrootar és bonic`.
  - `bo.+`[170]`b` coincideix amb **bo**`cs i ca`**b**`res` i amb **bo**`2`**b** però no amb `bob`.
  - `^root` només coincideix amb les línies que comencen per `root`.
  - `$root` només coincideix amb les línies que tenen `root` al final.
- Està orientat a caràctes[171].
- Normalment es processa per línies.
- S'utilitza molt: per a la substitució de caràcters en textos, per a canviar certs tipus de formats, cerca de paraules claus, etc.
- Alguns tokens:

167 L'argument -f1 extrau el primer camp de les files d'/etc/passwd i l'argument -d n'elimina els dos punts.
168 La primera columna del fitxer /etc/passwd conté els noms dels usuaris del sistema.
169 La comada expr serveix per a avaluar expressions regulars.
170 .+ tot junt significa “cincideix un o més caràcters”.
171 Per exemple és molt útil per a analitzar el pas de paràmetres en una comada de sistema.

Token	***Coincideix amb***
^	Inici de línia;
$	Final de línia;
.	Un caràcter qualsevol; a.c -> abc, axc, ...
[]	Rang o llista. c[a-z,O,Z] -> cap, cep, cOp, ...
[^]	Excepte rang o llista
\s	Caràcter espai
\S	No caràcter espai

- Comandes que utilitzen expressions regulars
  - grep -> aplica patrons a STDIN i en retorna els resultats per la STDOUT

Argument	***Acció***
-c	Llista els números de les línies que coincideixen
-I	Utilitza els partenrs de forma case insensitive
-v	Retorna les línies que no coincideixen
-w	Força que la coincidència s'estengui a tota la paraula
-x	Força que la coincidència s'estengui a tota la frase
-f nomfitxer	Passa nomfitxer com a llista de patrons[172]; ex: grep -f fitxerPatrons </etc/passwd

    - Exemples

```
$ cat </etc/passwd | grep root
```

  - Sed -> retorna per STDOUT el que se li passa per STDIN modificat.
    - Exemples:

```
$ sed s/root/wheel/g </etc/passwd[173]
$ sed 's/:.*$//' </etc/passwd[174]
```

  - awk ->

172Normalment les comandes accepten el paràmetre -e seguit de patró per passar tants patrons com es vulgui.
173Tots els patrons root els canviarà per wheel; sense la g només ho faria al primer.
174Llista tots els usuaris del sistema

Background i foreground

&	La comada s'executarà en background
Ctrl+Z	Envia a bacground el procés que s'està executant en foreground
fg	Comanda que retorna a primer pla un procés que s'estava executant en background
nice	Permet gestionar les prioritats d'execució dels processos en background
jobs	Mostra els processos que s'estan executant en background

Caràcters especials

Caràcter	***Significat***
~	Directori home[175]
`	Substitució de comanda[176]
#	Comentari
$	Expressió variable
&	Background job
*	Comodí de cadena
(	Inici d'una subshell
)	Final d'una subshell
\	[177] Literal el proper caràcter
|	Pipe
[	Inici d'un conjunt comodí
]	Fi d'un conjunt comodí
{	Inici de bloc de comanda
}	Fi de bloc de comanda
;	Separador de comandes de shell
´	Quoting fort
“	Quotin fluix
<	Redirector d'entrada

175 `echo $HOME`

176 Arcaic.

177 Precedirà qualsevol dels caràcters de la llista quan es vulgui que aquests siguin agafats literalment

Caràcter	*Significat*
>	Redirector de sortida
/	Separador de directoris al pathname
?	Un únic caràcter comodí
!	

Continuació de línia

\	Amb intro darrera fa que l'intro s'interpreti com a trencament de línia, i no com a fi de comanda.

Tecles de control

`stty all` retorna totes les tecles de control

Tecla de control	*Nom a stty*	*Funció*
Ctrl-C	intr	Interromp l'execució de la comanda
Ctrl-D	eof	Final de fitxer d'entrada
Ctrl-\	quit	Interromp l'execució de la comanda[178]
Ctrl-S	stop	Congela la sortida per pantalla[179]
Ctrl-Q		Continua la sortida per pantalla[180]
Ctrl-D	erase	Esborra l'últim caracter[181]
Ctrl-U	kill	Esborra la línia de comandes sencera
Ctrl-Z	susp	Deixa en suspensió la comanda actual

Compleció textual

- TAB

.bash_profile, .bash_logout, .bashrc i /etc/profile[182]

178Per quant Ctrl-C no funciona.
179Desfasat.
180Desfasat.
181Tal i com fa DEL
182Qualsevol script corre en una subshell. Per tant, si es vol que les variables que es defineixen en els scripts inicials siguin visibles al la sessió interactiva caldrà que siguin exportades (`export`) a aquesta sessió, que és la sessió pare.

- Serveixen per tunejar l'entorn d'usuari

.bash_profile[183]	Script que s'executa després de cada login.
.bash_logout	Script que s'executa abans de sortir de bash amb exit o logout.
.bashrc	Script que s'executa cada cop que comença bash[184].
/etc/profile	Com .bash_profile però per a tots els usuaris[185].

Alies

- Per crear comandes noves.

  Per exemple: `alias ls='ls --color=auto'`

Variables

- Amb `export` es fan accessibles a les shells pares.
- Bash posa èmfasis especial en les variables basades en cadenes de caràcters

VARIABLE[186]=valor	Assigna valor a variable[187]
${VARIABLE}[188]	Retorna el valor de variable

Variables de prompt	
PS1	Prompt primari
PS2	Prompt secundari; quan es trenca una línia amb \
PS3	Per a programació de la shell
PS4	Per a debugar

183O també .bash_login.
184Es pot, per exemple, des del mateix bash executar `bash` s'obrirà una subshell a on s'haurà executat el fitxer .bashrc.
185Només l'ha de poder modificar el root.
186Per conveni les a variables de shell se'ls dóna noms en majúscules.
187També accepta arrays unidimensionals: GRUP1=([6]=martí [9]=lola). Per a la consulta ${nomvariable[index]}.
188Es pot utilitzar la versió simplificada $VARIABLE.

Variables d'entron[189] principals	
TREM	Tipus de terminal que s'utilitza
SHELL	Camí absolut a la shell (/bin/bash)
HOME[190]	Camí absolut al directori de home de l'usuari
USER	Nom de login
DISPALY	Direcció al servidor X
PWD	Directori actual

-	Directori anterior a l'actual
?	Últim valor (d'error) retornat

umask

- Per establir els permisos per defecte dels fitxers que es creen.
- Permisos que tindrà el fitxer = permisos que assigna el procés creador del fitxer NAND valor d'umask

  Exemple: si l'umask és 022 implica que els permisos màxims que podrà tenir un fitxer en ser creat seran 755 (777[191] NAND 022); si el procés que crea el fitxer[192] els assigna per defecte els permisos 666, els permisos finals que tindrà el fitxer seran 644 (755 AND 666).

Programació de Bash

- Es pot fer:
  - per línia de comandes
  - per fitxer -> s'executa en una subshell
    - La primera línia sempre serà #[193]!/bin/bash

189La comanda env les mostra totes i els valors a què estan assignades.
190El caràcter especial ~ és sinònim de la variable.
191Permisos màxims equivalents a `rwxrwxrwx`.
192Un editor de text, per exemple.
193Tot i que en general # deixa sense efecte la resta de la línia que hi ha a la seva dreta, aquest cas és una excepció que serveix per a indicar a on es troba el programa que es farà càrrec, en aquest cas interpretarà, la resta del contingut del fitxer.

Jerarquia de preferències

1. alies
2. paraules clau tals com function, if i for
3. funcions
4. built-ins
5. scripts i programes binaris

Funcions

- A diferència dels scripts, les funcions corren dins del mateix procés des d'on han estat invocades.
- Són útils perquè:
  - queden en memòria => velocitat d'accés ràpida
  - permeten fer els scripts més intel·ligibles
- Formes de definir-les[194]:
  - ```
    funciton nomFuncio {
          comandes de shell
    }
    ```
  - ```
    nomFuncio () {
          comandes se shell
    }
    ```
- Per eliminar una funció que hi ha en memòria:
  - `unset -f nomFuncio`
- Per llistar les funcions que hi ha en memòria:
  - `typeset -f`
- Per veure el codi d'una funció:
  - `type`[195] `-all nomFuncio`

194No hi ha cap diferència entre les dues.

195També és útil per a conèixer el tipus d'una comanda. Per exemple:

```
$ type -type bash
file

$ type -type if
keyword
```

Variables

Paràmetres posicionals	Significat
$*	Tots els paràmetres posicionals[196]
$@	“$1” “$2” “$3” ...
$0	Nom de l'script que l'ha invocat
$1, $2, etc.	Arguments que s'han passat a l'script

Operadors de cadenes

- Són útils per:
    - Garantir que una variable existei[197].
    - Establir els valors per defecte de les variables.
    - Detectar errors resultants de variables no assignades
    - Eliminar porcions de variables que coincideixen amb patrons

Sintaxi d'operadors de cadenes	
Operador	Substitució
${nomVariable:-paraula}	Si nomVariable existeix i és no nul·la, retorna el seu valor; sinó retorna paraula.
${nomVariable:=paraula}[198]	Si nomVariable existeix i és no nul·la, retorna el seu valor; sinó l'assigna a paraula retorna aquest valor.
${nomVariable:?missatge}	Si nomVariable existeix i és no nul·la, retorna el seu valor; sinó imprimeix el valor de nomVariable seguit de missatge i aborta l'execució de la comanda o l'script.
${nomVariable:+}	Si nomVariable existeix i és no nul·la, retorna el seu valor; sinó retorna nul.

Patrons i coincidència de patrons

- Són útils per eliminar components dels paths dels fitxers

196Separats pel separador de camps intern (IFS): espai, TAB i NEWLINE.
197Per tan que ha estat definida i assignada a un valor no nul.
198Els paràmetres posicionals i ells especials no es poden assignar per aquest mètode.

Sintaxi d'operadors de coincidència de patrons	
Operador	Significat
${nomVariable#patró}	Si el patró coincideix amb l'inici del valor de nomVariable, esborra la part més curta que conicideix, i retorna la resta.
${nomVariable##patró}	Si el patró coincideix amb l'inici del valor de nomVariable, esborra la part més llarg que conicideix, i retorna la resta.
${nomVariable%patró}	Si el patró coincideix amb el final del valor de nomVariable, esborra la part més curta que conicideix, i retorna la resta.
${nomVariable%%patró}	Si el patró coincideix amb el final del valor de nomVariable, esborra la part més llarga que conicideix, i retorna la resta.

Substitució de comandes

Sintaxi de la substitució de comandes	
$(comandaUNIX)	Executa comandaUNIX

Exmple: `echo $(ls $(pwd))` treu per pantalla la llista de fitxers del PWD.

Control de flux

- Totes les comandes de UNIX quan acaben retornen un número:
  - 0 si la comada ha finalitzat correctament[199]
  - 1-255 si hi ha hagut algun error d'execució[200]

- `return valor` -> serveix per retornar valor i sortir.

Comprovació dels atributs de fitxer[201]	
-d fitxer	fitxer existeix i és un directori
-e fitxer	fitxer existeix
-f fitxer	fitxer existeix i és un fitxer regular[202]

199Habitualment.
200El número serveix per a identificar l'error.
201N'hi ha més d'una vintena en total.
202Per tan no és ni directori ni cap altre tipus de fitxer especial.

Comprovació dels atributs de fitxer	
-r fitxer	Tens permisos de lectura sobre fitxer
-s fitxer	fitxer existeix i no és buit
-w fitxer	Tens permisos d'escriptura sobre fitxer
-x fitxer	Tens permisos d'execució sobre fitxer[203]
-O	El fitxer et pertany

Condicionals enters[204]	
-lt	Menor que
-le	Menor o igual que
-eq	Igual que
-ge	Major o igual que
-gt	Major que
-ne	No igual

`if/else`

- sintaxi:

```
if condició
then
     sentències
[elif condició
     then sentències]
[else
     sentències]
fi
```

- aprofitant el retorn de les comandes per avaluar la condició:

```
if la comanda ha finalitzat correctament
then
     sentències per al procediment normal
else
     sentències per a l'error
fi
```

El retorn de variables es poden operar ralacionals (<, >, ==, !=, &&, ||)

`for`

203Si fitxer és un directori es tradueix en tenir permisos per buscar-hi.
204No s'ha de confondre amb > o >, que fan comparacions lexicogràfiques.

- sintaxi:

```
for x := 1 to 10 do
begin
     sentències
end
```

- per treballar amb llistes:

```
for nom [in llista]
begin
     sentències a on es pot utilitzar $nom
end
```

altres construccions de control de flux: `case, select, while, until`

Hello, world!

```
$ cat > hello.sh << "EOF"
> #!/bin/bash
> echo "Hello, world!"
> EOF
$ chmod 755 hello.sh
./hello.sh
Hello, world!
```

```
$ cat > hello1.sh << "EOF"
> echo "Hello, world!"
> EOF
$ source hello1.sh
Hello, world!
```

Comandes principals de sistema[205]

Consulta documentació

- man[206] - Mostra el manual del nom que se li ha passat com a paràmetre

```
$ man man          -> mostra la secció 1 (comandes de sistema) del
                      manual de man
$ man 7 man        -> mostra la secció 7 (miscel·lània i convencions)
                      del manual de man
```

  - És recomanable llegir atentament les man pages i tot el seu contingut, ja que són textos molt condensats i treballats.

  - Cal llegir les man pages (man(1) i man(7)) per entendre què són les man pages i com estan estructurades.

205 Es recomana que es llegeixin totes les man pages i les info de les comandes que es presenten a continuació, ja que cal conèixer-les bé, amb les seves opcions principals incloses.

206 Utilitza les variables d'entorn MANPAGER, per a establir el paginador a utilitzar, i MANPATH, per establir els directoris a on cal cercar la informació.

- Info[207] - Per a consultar les info[208] dels programes

man vs. info	
man	**info**
Normalment formatats amb groff[209]	Preformatats des de texinfo
Covertura concisa de l'ús i de les opcions	Guies d'usuari extenses i documentades
Els links es fan per mitjà de referències de text	Suport integrat d'hipervincles
Organitzades per seccions i per nom de programa o de funció	Organitzades per nom de paquet o de programa
Fitxers petits	Fitxers gran
No trivials de generar	Ús de tags

Actualment GNU genera les man pages des de les info[210].

- Apropos – Per a buscar paraules clau en al conjunt de les seccions de descripció de les man pages; en mostra les entrades que les contenen.

Gestió de fitxers

- ls – llista els fitxers amb el criteri: [0-9], [A-Z], [a-z].
- cp – copia fitxers.
  - La sintaxi és estricta: cp origen1 origen2 ... destí[211].

    `$ cp /etc/passwd .`[212] -> copia el fitxer /etc/passwd al directori de treball.
- rm – esborra fitxers.
- mv – mou fitxers, és a dir, primer copia i després esborra la font.
- mkdir – crea directoris.

207Aquest sistema de documentació el genera GNU argumentant la inexistència d'una eina open source per a man i que a més a més el sistema en si no és eficient per a generar documentacions grosse. Es tracta, sens dubte, d'una tecnologia molt més potent i fonamentada

208pinfo és una aplicació per al visionat de pàgines info en color.

209Curiosament, durant el procés de solució de la inexistència d'una eina per gestionar mans, GNU crea la implementació de roff (sistema estàndar de UNIX per al formatat de documentació) que s'ha convertit en estàndard.

210Mitjançant el programa help2man.

211No especificar el destí pot tenir conseqüències desastroses.

212El punt especifica al directori actual; dos punts seguits indica el directori pare de l'actual.

- find – busca fitxers.
- which – retorna el camí al fitxer que s'executarà si es tecleja a la línia de comandes.
- tar – fa/desfà tarballs[213].
- gzip – compressor/descompressor d'arxius[214].
- bzip2 – compressor/descompressor d'arxius[215].
- touch – modifica les dades temporal d'accés als arxius[216].
- xargs – construeix una llista d'arguments que es passarà a la comanda que l'acomapanya[217].

Continguts dels arxius

- file – estableix el tipus d'arxiu[218].
- cat – retorna per l'STDOUT el contingut dels fitxers.
- head – retorna per l'STDOUT les primeres línies dels fitxers.
- tail– retorna per l'STDOUT les últimes línies dels fitxers.
- cmp – retorna per l'STDOUT el resultat de la comparació d'arxius de qualsevol tipus.

---

213 Els tarballs són fitxers que contenen estructures de directoris amb els corresponents fitxers. Són molt útils a l'hora de manipular estructures de directoris, ja que estalvien l'haver d'utilitzar recursos recursius.
L'extensió utilitzada en aquest tipus d'arxius és la .tar.
Habitualment, cara al magatzematge de dades (backup), després de crear el tarball que conté les dades, se li aplica un algoritme de compressió per obtenir un arxiu més reduït.

214 L'extensió utilitzada en aquest tipus d'arxius és la .gz. Si el contingut és un tarball, es reconeixen per .tar.gz o .tgz de manera abreviada.
La combinació de gzip amb altres comandes com ara cat, less, cmp, apareixen les comandes que es coneixen amb el nom de ztools, que permeten accedir al contingut dels fitxers comprimits, sense necessitat d'haver de descomprimir-los explícitament per la línia de comandes. Algunes ztools poden ser: zcat, zless, zcmp, etc.

215 L'extensió utilitzada és la .bz2.
Normalment l'algoritme de bzip2 dóna més bons resultats quan a compressió; tot i això, gzip és força utilitzat, sobretot per motius històrics.

216 També es pot utilitzar per a generar un arxiu buit fins a les hores inexistent al directori de treball.

217 Per exemple `find . -type f | xargs chmod 644` busca tots els fitxers regulars del directori actual i dels seus subdirectoris i xargs els llista perquè chmod els assigni els permisos 644

218 La tècnica usada es basa en els “magic numbers” (`man 5 magic`); a cada tipus d'arxiu se li associa un nombre per a la seva identificació, el qual forma part dels continguts del propi arxiu. Hi ha tipus d'arxius que necessiten tècniques especials (per exemple els binaris)

- diff – retorna per l'STDOUT el resultat de la comparació d'arxius de text pla[219].
- more[220] – mostra per pantalla el resultat de l'aplicació de la paginació sobre un arxiu.
- less[221] – mostra per pantalla el resultat de l'aplicació de la paginació sobre un arxiu.
- tee – multiplexa l'entrada sobre les diverses sortides especificades[222].

Manipulació de dades. Filtres.

- cut – elimina parts de les línies dels arxius.
- sort – ordena les línies de sortida.
.
- sed – l'editor de línia.
- grep – el cercador de patrons en les línies d'entrada.
- tr – el traductor de caràcters.

Dispositius d'emmagatzematge

- mount – afegeix/extreu dispositius del filesystem.
- df – estadístiques d'espai lliure.
- du – estadístiques d'ús dels dispositius.

Processos

- ps – estat dels processos[223].
- top – mostra informació actualitzada i ordenada dels processos del sistema.
- kill – senyals per a finalitzar un procés pel PID.

219Aquesta comanda és la que s'utilitza per a la generació/aplicació de patchs.
220Aquest tipus d'aplicacions es coneixen amb el nom de paginadors.
221less és molt més complet que more. Tot i això, normalment less no forma part dels sistemes mínims, mentre que per aquests, genaralment, more és el paginador per defecte.
222$ tee <original.txt replica1.txt replica2.txt
223Els processos s'identifiquen pel PID (Process ID)
Els scripts dels serveis acostumen a emmagatzemar el seu PID a /var/run/nomdeservei.pid per controlar el procés associtat.

- killall – senyals per a finalitzar un procés identificat pel nom.

Informació

- uname – informació del sistema.
- id – Identificació de l'usuari.
- who – usuaris del sistema.
- w – usuaris del sistema i què fan.
- date – establiment/consulta de l'hora i dia del sistema.
- dmesg – mostra el contingut.

Aturada del sistema

- halt – aturada del sistema.
- reboot – reengegada del sistema
- shutdown – aturada d'un servidor.

Canvi de runlevel

- init – canvi de runlevel.

Sistema de fitxers

Filesystem Hierarchy Standard (FHS[224])

- UNIX[225] és un sistema fortament estructurat, i convé seguir-ne sempre els estàndards; també pel que fa als directoris del sistema:

224 http://www.pathname.com/fhs

225 De fet, però, no hi ha cap sistema Linux que compleixi al 100% les especificacions FHS, sobretot degut a l'arcaisme del kernel, i del procés d'engegada, el qual tampoc s'ha resolt d'acord amb les especificacions FHS. Per exemple, l'/etc/mtab, el qual hauria d'estar, per definició a /var/ per ser un fitxer dinàmic dependent de mount, ha d'estar a /etc/ ja que ha d'estar disponible just després de muntar-se el root filesystem.

Directori	***Observacions***
/	Directori arrel o root. No ha de tenir més subdirectoris que els que té per defecte.
/boot/	Conté tots els fitxers del bootloader, els de configuració inclosos, i opcionalment els kernels.
/etc/	Directori per a la configuració específica del host. Qualsevol fitxer[226] que s'hagi de modificar per adaptar configuracions ha d'anar a aquest directori o als seus subdirectoris.
/home/	Dades d'usuari
/mnt/	Filesystems muntats temporalment[227].
/usr/	Dades i programari compartits de només lectura. Per tant, excepte durant els processos d'upgrade, aquest directori hauria de poder ser muntat com de només lectura i no hauria de representar cap problema[228].
/usr/lib/	Recursos dependents de l'arquitectura. Arxius necessaris per al sistema que depenen de l'arquitectura, inclosos els binaris.
/usr/local/	Recursos i programari específic[229].
/usr/share	Recursos independents de l'arquitectura.
/tmp/	Dades temporals, la persistència de les quals no està garantida entre processos diferents[230].
/var/	Dades “transitòries”; l'àmbit de treball del sistema a on s'emmagatzemen fitxers per al control, logging, caching, i d'altres funcions administratives.
/var/log/	Tots els logs del programari de Debian emmagatzemen el log aquí.
/var/mail/	Si l'MDA local utilitza el format mailbox, els mailbox dels usuaris són en aquest subdirectori.
/var/tmp/	

Directoris addicionals de Debian

Directori	***Observacions***
/media/	Dispositius de magatzematge que es poden extreure, com ara CDROMs, llapis USB, etc.

226Com a excepció els del grub són a /boot/grub/.
227En teoria, aquest directori només hauria de ser utilitzat per a l'administrador per a muntar fs temporals. Per tant, els dispositius de magatzematge massiu no haurien de ser muntats aquí; Debian proporciona el directori /media/ per aquesta finalitat.
228Habitualment el /usr/src/ es fa servir per allotjar les fonts del kernel; això fa que per compliar-lo al menys aquest subdirectori hagi de tenir permisos d'escriptura (també es pot considerar aquest procés com a un procés d'upgrade).
229Aquí hi va el programari que no és de Debian; Debian mai toca aquest directori.
230En molts sistemes a l'hora d'aturar-se es perd la informació d'aquest directori.

Directori	***Observacions***
/srv/	Dades de servidor. Totes les dades que proveeix el sistema en els seus serveis com a servidor.

Perl[231]

- Llenguatge que està entre els llenguatges de baix nivell i els d'alt nivell (per exemple entre C i Bash).
- Basat en expressions regulars => elimina molta sintaxi.
- Pensat per a l'administrador, el qual necessita que la feina es faci, sense preocupar-se massa de formalismes.
- Sempre es necessita que l'interpretador/compilador formi part de sistema, ja que el codi es precompila[232] just abans de cada execució[233].
- La tècnica de precompilació permet obtenir rendiments pròxims als dels binaris purs[234] i els avantatges dels llenguatges d'scripting.
- Permet, per ell sol, obtenir resultats que en Bash requeririen l'awk i el sed[235].
- Sobresurt per la seva eficiència a l'hora de manipular fitxers de text.
- Hi ha gran quantitat d'scripts de Perl open source llestos per a ser estudiats i utilitzats[236].
- L'ús de flags a l'hora d'invocar l'script serveixen per modificar el comportament de l'interpretador.
- Buit-in warnings[237]: per ajudar a la depuració:
    - `$ perl -w rutaPrograma`

231 Acrònim de practical extraction and report language.

232 Per obtenir el que es coneix com a bytecode, estructura de dades internes que representen el programa. En el modus operandi de Perl no té sentit emmagatzemar el bytecode per a futures execucions, com podria ser en el cas dels binaris de C; tot i això s'esperen variacions importants en aquest camp cara la versió 6 de Perl.

233 La presència de bucles interns no significa una penalització computacional , ja que només es compilen un cop, i s'executen n vegades.

234 Per exemple els generats a partir de codi C amb el compilador.

235 De fet hi ha qui diu que Perl és la navalla suïssa de l'administrador, ja que conté tot allò necessari per a solucionar la majoria de problemes.

236 Per exemple a http://www.cpan.org s'intenta recopilar tots aquests scripts.

237 També es poden trobar encastats a la segona línia de programa: `use warnings; use diagnostics;`

- `$ perl -Mdiagnostics rutaPrograma`

- Tipus de variables principals:

Tipus	***Símbol***	***Ús***
escalar	$	Un únic enter o cadena
Array/llista	@	Grup de dades indexades per un enter
Hash	%	Grup de dades indexades per qualsevol escalar
Filehandle	(no en té)	Per a accedir a fitxers oberts

- Les variables no estan inicialitzades per defecte[238].

- Assignació de variables:

  TipusNomdevar = valor;

- Contextos

  - Serveixen per “acabar de perfilar el comportament” de les variables

Operador	***Context***
+	Numèric
.	Cadena
	“don't care” o booleà

- Exemples:

```
$var1 = 10;
$var2 = “20”;
$resultat1=$var1+$var2; # -> 30
$resultat2=$var1.$var2; # -> 1020
```

- Filehandles i fitxers

```
open (SORTIDAORDENADA, “|sort >[239] /tmp/ordenat.txt”);
open (SORTIDAORDENADA, “ls -R|”);
close (SORTIDAORDENADA);
close (LLISTADARXIUS);
```

- Captura de l'entrada per teclat: filehandler <STDIN>

238Es pot emprar la funció undefined() per a comprovar si una variable està o no inicialtizada.

239> indica obertura per sobreescriptura; >> obertura per afegir al final; < obertura per només lectura; +< o +> obertura per lectura i escriptura sense pèrdua de continguts.

```
print “Quants anys tens?\n”;
$edat = <STDIN>[240];
print “Tens $edat anys!”;
```

Hello, world!

```
$ cat > hello.pl << "EOF"
> #!/usr/bin/perl
> print "Hello, world!\n";
> EOF
$ chmod 755 hello.pl
./hello.pl
Hello, world!
```

```
$ cat > hello1.pl << "EOF"
> print "Hello, world!\n";
> EOF
$ perl hello1.pl
Hello, world!
```

240També es pot fer amb <>.

4t Capítol: Administració local

Conceptes bàsics de seguretat

- La seguretat és una qüestió d'estratègia integral
- La seguretat total és impossible => construir “sistemes defençables” a on s'accepten derrotes parcials

Definicions de seguretat

1. Visió **dinàmica** de la seguretat:
    - plantejament general
    - procés continu a on s'hi poden distingir quatre fases:
        I. **Avaluació**-. Anàlisi dels requeriments i de l'entorn dels sistema:

            -> es genera el document de política de seguretat

            -> s'especifica com s'implementarà aquesta política

        II. **Protecció**-. Implementació del sistema

        III. **Detecció**-. Identificació d'atacs i violacions de la política de seguretat:

            -> monotorització

            -> anàlisi de logs

            -> detecció d'intrusos

        IV. **Resposta**: actuació d'acord amb el pla de seguretat establert
2. Concepció **estàtica** de la seguretat: tècniques concretes
    - tres/quatre aspectes capitals per a la **informació** (emmagatzemada o en transit) i per als **recursos**:
        I. **Confidencialitat**-. no pot ser accessible per parts no autoritzades

II. **Integritat**-. ha de romandre inalterada fins que no la canviï una part autoritzada

III. **Disponibilitat**-. ha d'estar sempre disponibles a les parts autoritzades, sense interrupció de servei

IV. **Registre (accountability)**-. sempre s'ha de registrar què fa cadascú

Principis essencials de seguretat

- **Simpliciat**-. cal dur sempre a la pràctica el principi de simplicitat
- **Compartimentalització**-. per poder isolar les parts afectades
- **Fallida segura**-. cal garantir que si un component falla ho fa de manera segura[241]
- **La baula més feble**-. cal posar l'atenció per millorar aquella part de sistema que sigui la més feble
- **Principi del privilegi mínim**-. cada part del sistema ha de tenir només aquells privilegis que siguin imprescindibles per poder fer la tasca que ha de fer
- **Servei mínim**-. només s'ha de donar aquells serveis que se'ns exigeixen, ja que cada servei que s'afegeix significa obrir la porta a possibles vulnerabilitats
- **Secretisme[242]**-. no s'ha de permetre l'accés a dades que informin sobre les estratègies de seguretat implementades

Atacs	***Respostes/Prevenció***
Denegació de servei[243] (DoS)	Estar preparat per a rebre aquests atacs.

241 Per exemple, davant d'una fallida del sistema de validació cal garantir que el sistema respondrà no deixant validar a ningú, i mai permetent l'accés descontrolat.
242 Segons algunes fonts bibliogràfiques.
243 Hi ha autors que asseguren que aquest tipus d'atac constitueix entorn del 90% del total dels atacs.

Atacs	***Respostes/Prevenció***
Denegació de servei distribuït[244] (DDoS)	
Explotació d'errors de configuració	Una instal·lació inicial segura Planificar els canvis i avaluar el seu impacte abans d'implementar-los.
Explotació de vulnerabilitats d'Apache	Estar al cas de les actualitzacions.
Explotació de vulnerabilitats de l'aplicació	Avaluar i provar l'aplicació abans de posar-la en producció.
Explotació d'altres serveis	No donar més serveis que els estrictament necessaris.

Identificació

PAM – Pluggable Authentication Modules

- Unifica i proveeix mètodes per a (regles estàndard):
  - l'autenticació -> /etc/pam.d/common-auth
  - inicialització de compte -> /etc/pam.d/common-account
  - inicialització de sessió -> /etc/pam.d/common-session
  - canvi de password -> /etc/pam.d/common-password
- Els pot usar una aplicació sola o un grup de programes
- Permet l'ús combinat de diversos mètodes d'autenticació
- Els serveis particulars (login, su, xscreensaver, etc.) imposen les seves regles particulars, i incorporen les estàndards mitjançant `@include`

/etc/passwd
adduser, useradd, bla
Shadow Password

MD5

244Diversos nodes zombi amb accés a internet per banda ampla, a les ordres d'un node mestre governat per l'atacant, llancen tantes peticions de servei com poden contra el/s node/s objectiu. Normalment els nodes llancen les peticions en nom de nodes externs per evitar rebre el tràfic resultant de les peticions.
La segona setmana de febrer de l'any 2000 és coneguda com a setmana negra dels atacs DDoS, ja que els servidors de diverses institucions, com la CNN, Yahoo (el buscador més utilitzat en aquells moments) o e-bay, entre d'altres, van quedar fora de servei durant diverses hores per ser objecte d'atacs DDoS llançats des d'ordinadors de la universitat de Califòrnia.
A http://staff.washington.edu/dittrich/misc/ddos/ hi ha molts links sobre DDoS.

sudo

- Permet la gestió de privilegis dels usuaris[245].

Sistemes d'emmagatzemament de dades i backups

- tar, cp -a, scp

RAIDs software - mdadm[246]

- Tipus de RAID més usuals
    - Lineals
        - “Un hdd al costat dels altres”
        - Es sumen les capacitats
        - Els discs no han de ser iguals
        - Els discs es van omplint l'un darrera l'altre
        - No hi ha redundància.
        - En cas de fallada pot ser que es puguin recuperar dades
    - RAID0
        - “Un hdd al costat dels altres”
        - Es sumen les capacitats
        - Els discs no han de ser iguals[247]
        - Els blocs es van escrivint a un disc i a l'altre => augmenta les velocitats d'accés
        - No hi ha redundància.
        - En cas de fallada en cap cas es pot recuperar dades
    - RAID1
        - “Un disc fa de mirall de l'altre”[248]
        - La capacitat del RAID serà igual a la del disc més petit
        - Les velocitats d'accés disminueix
        - Hi ha redundància
        - En cas de fallada d'un hhd, el sistema es recupera automàticament
    - RAID5
        - Els discs treballen de forma cooperativa

245És una bona alternativa a l'ús indiscriminat de la compta root.
246El projecte raidtools també permet la gestió de raids, però està quedant obsolet.
247Quan s'accedeixi a la part del disc dur gran que no té mirror, el rendiment baixa.
248Es pot fer amb més de dos discs, per augmentar-ne la redundància.

- La capacitat màxima del RAID és (N-1)*S; N nombre de discs, S capacitat del disc més petit
- Les velocitats d'accés augmentent[249]
- Si un disc falla, s'inicia immediatament el procés de reconstrucció del RAID i no es perden dades
- Si durant el procés de recuperació del RAID falla un altre disc, es perden totes les dades.
- Un cop finalitzat el procés de recuperació el RAID torna a ser immune a la fallada d'un disc.

Gestió de dispositius lògics - LVM

- Facilita la tasca d'assignació de recursos a usuaris i aplicacions
- Es pot fer modificacions a les assignacions sense perdre dades
- Es pot muntar sobre un RAID software

Eines gràfiques d'administració - WebAdmin

Programari no debianitzat

- És recomanable utilitzar sempre programari debianitzat per deixar en mans dels gestor de paquets les tasques relacionades amb les dependències.
- Si un programari no està debianitzat:
    1. Obtenir el codi font
    2. Desempaquetar-lo
    3. Llegir la documentació que porta
- Procediment habitual de complilació:

```
$ ./configure [paràmetres addicions[250]]
```
-> per generar el MAKEFILE

```
$ make
```
-> per compilar el codi font

249Tot i que es fa difícil predir com ho fan.
250Un dels habituals és --prefix /ruta/a/on/s'instal·larà/el/programari/.

```
# make install[251]
```
-> per integrar els binaris al sistema

Kernel

Recompilació estàndard del kernel[252]

1. Obtenir les fonts d'algun mirror oficialment idesempaquetar-les:

```
# cd /usr/src/

# wget ftp.rediris.es/mirror/kernel/linux/kernel/v2.6/linux-2.6.15.tar.bz2[253]
f
# tar xjf linux-2.6.15.tar.bz2

# cd linux-2.6.15
```

   - Si es vol evitar haver de descarregar totes les fonts senceres cada cop que apareix un nucli nou, es pot baixar únicament el patch corresponent i aplicar-lo[254] a les fonts antigues per actualitzar-les.

2. Si es vol utilitzar la configuració del kernel del sistema es copia al lloc pertinent; s'entra al menú de configuració[255], s'efectuen els canvis, es desa la configuració i es surt del menú.

```
# cp /boot/config-2.6.15-486 .config

# make menuconfig
```

3. Es compila

```
# make
```

4. Es compila tot i s'instal·len els mòduls

```
# make all && make modules_install
```

5. Es copia el nucli creat al directori /boot/[256]

```
# cp arch/i386/boot/bzImage /boot/vmlinuz-2.6.15
```

---

251 Habitualment requerirà permisos de root.

252 Per a kernels 2.6. Pels 2.4 és diferent.t

253 També es pot fer amb una sessió interactiva d'ftp, per exemple amb el client lftp.

254 En aquest cas, per actualitzar de 2.6.14 a 2.6.15 es descarrega el patch patch-2.6.15.gz a /etc/src/, s'entra al directori a on hi ha les fonts del 2.6.14 i s'executa: zcat ../patch-2.6.15.gz | patch -p1.
Per a utilitzar patch caldrà tenir el paquet patch instal·lat.

255 Per això cal tenir instal·lats els paquets següents: make, gcc, gcc-4.0, binutils, lib6-dev i libncurses5-dev.
Sempre es pot utilitzar l'script de comprovació de compliment dels requeriments mínims del sistema, /usr/src/linux-2.6.15/scripts/ver_linux.

256 En aquest directori també es poden crear subdirectoris per a ordenar els seus continguts

6. Es copia el fitxer System.map[257] generat al directori /boot/[258]

   ```
   # cp System.map /boot/System.map-2.6.15
   ```

7. Es genera la imatge del sistema de fitxers[259] que carregarà al ramdisk el grub

   ```
   # mkinitrmafs -k -o /boot/intrd.img-2.6.15 2.6.15
   ```

8. Es modifica convenientment la configuració del grub[260]. A mode d'exemple:

   ```
   # /boot/grub/menu.lst

   title      Debian GNU/Linux, kernel-2.6.15
   root       (hd0,6)
   kernel     /boot/vmlinuz-2.6.15
   initrd     /boot/initrd-2.6.15
   savedefault
   boot
   ```

Recompilació del kernel mitjançant les eines de Debian[261]

- Com a resultat s'obté un paquet .deb que conté tots els arxius necessaris per a la instal·lació del nous kernel.
- Es fa mitjançant les eines del paquet kernel-package[262].

1. Es descarreguen les fonts, s'entra al seu directori, i es genera el .config
2. S'utilitza make-kpkg per a la compilació del kernel i la creació del paquet .deb

   Per crear el paquet kernel-image-2.6.15-1:

   ```
   # make-kpkg -rev 1 kernel_image
   ```

   Per crear el paquet amb els headers:

   ```
   # make-kpkg -rev 1 kernel_headers
   ```

257 Aquest fitxer conté la taula de símbols del kernel, juntament amb el “fitxer” /proc/ksyms.
258 Estrictament no caldria fer-ho ja que en el procés de boot aquest fitxer també es busca a /usrc/src/linux/, però això significa que qualsevol canvi d'aquest symlink (el qual duran el procés de recompilació del kernel exposat aquí ni s'ha creat perquè no és necessari) conduirà a un System.map erroni
259 Aquesta imatge conté el sistema de fitxers mínim que necessita el kernel per poder muntar la resta de sistemes de fitxers.
260 És bona estratègia fer una inicialització dels paràmetres de manera general al principi del fitxer i a cada entrada assignar-los els valors adequats.
261 És per aquest mateix procediment que es generen els paquets dels kernels dels repositoris oficials.
262 El qual addicionalment necessita els paquets dpkg-dev i patch.

3. Per instal·lar el paquet del kernel que s'acaba de crear:

```
# dpkg --install kernel-image-2.6.15-1
```

4. Si es vol que grub mostri l'opció del kernel nou automàticament:

   - Cal crear el fitxer /etc/kernel-img.conf amb el contingut:

     postinst_hook =/ sbin/update-grub
     postrm_hook = /sbin/update-grub
     do_bootloader = no

Creació de paquets de mòduls no presents al kernel amb Debian[263]

module-assistant

Gestió de mòduls

lsmod-. llista els mòduls carregats

modprobe[264]-. gestiona els mòduls del kernel de forma intel·ligent

modinfo-. dóna informació del mòdul.

modconf[265]-. carrega mòduls mitjançant una interfície basada en ncurses

insmod-. carrega el mòdul al kernel

rmmod-. treu el mòdul del kernel

/etc/modules-. llista de mòduls que es carregaran durant l'arrancada del sistema

/etc/modprobe.conf /etc/modprobe.d/-. sistema de configuració de modprobe

/lib/modules/`uname -r`-. mòduls disponibles per a la versió del kernel

263Aquest és el mecanisme que s'utilitza per a crear els mòduls dels repositoris de Debian.
264Es recomana utilitzar sempre que sigui possible aquesta comanda front-end enfront de insmod, rmmod i altres comandes.
265S'ha d'instal·lar el paquet modcon

5è Capítol: Administració de xarxa

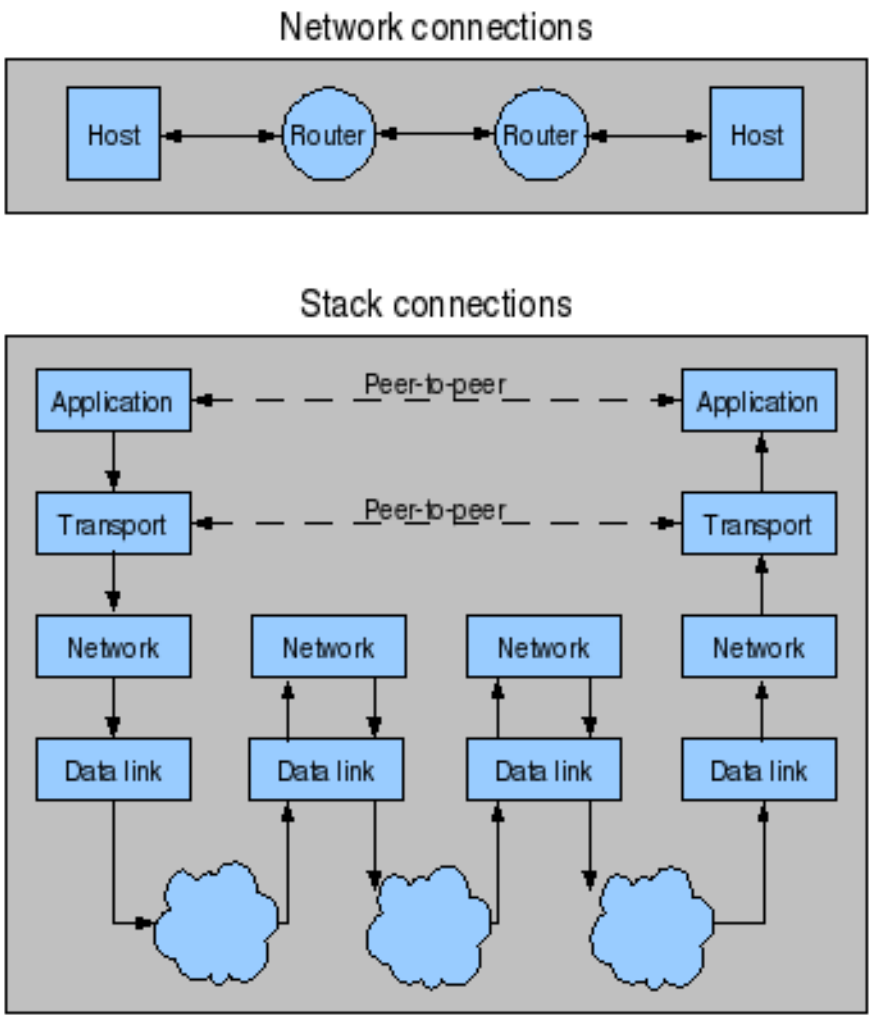
Piles

Internet Protocol Suite[266]		***OSI model***	***Protocols***
Aplication		Application	HTTP, SMTP, SNMP, FTP, Telnet, SIP, SSH, NFS, RTSP, XMPP, Whois, ENRP
		Presentation	XDR, ASN.1, SMB, AFP, NCP
Aplication/Transport		Session	ASAP, TLS, SSH, ISO 8327 / CCITT X.225, RPC, NetBIOS, ASP, Winsock, BSD sockets
Transport		Transport	TCP, UDP, RTP, SCTP, SPX, ATP, IL
Internetworking		Network	IP, ICMP, IGMP, IPX, BGP, OSPF, RIP, IGRP, EIGRP, ARP, RARP, X.25
Link	MAC	Data link	Ethernet, Token ring, HDLC, Frame relay, ISDN, ATM, 802.11 WiFi, FDDI, PPP
	Physical	Physical	Cable, radio, fibra òptica

Capes model TCP/IP	***Unitat de comunicació TCP***	***Unitat de comunicació UDP***
Aplicació	stream	message
Transport	segment	packet
Internet	datagrama	
Accés a xarxa	frame	

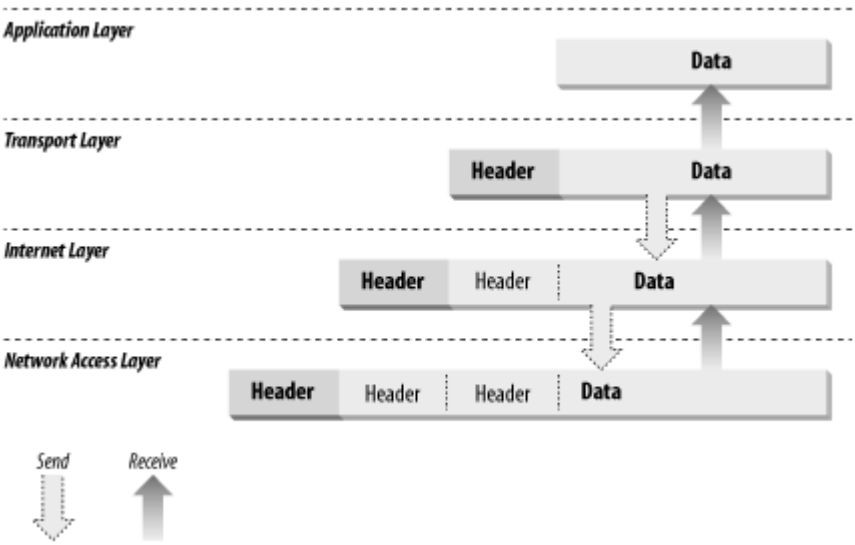
Protocol-. Conjunt de regles que governen la **sintaxi**, la **semàntica** i la **sincronització** d'una comunicació.

266Per aquest model la proposta de capes, en nombre i continguts, varia segons l'autor; aquesta inconsistència no es dóna en el model OSI.
De vegades també se'l coneix com a TCP/IP protocol suite en referència als dos protocols més importants que en formen part.



Font: http://en.wikipedia.org/wiki/Image:IP_stack_connections.png

Intervenció de les diferents capes en el procés de comunicació entre dos nodes



Font: TPC/IP Networking Administration, Craig Hunt. O'Reilly.

Exemple d'encapsulament.

- Estratègies d'emissió: Per a qui és el missatge?
    - Unicast – és per a un sol node

        -> és senzilla.

        -> és l'estratègia que es va desenvolupar i implementar primer per a la capa de transport.

        -> exemples: SSH, FTP, etc.

    - Multicast – és per a més d'un node, però no per a tots els nodes

        -> no és trivial[267]

        -> una solució possible és l'ús d'una adreça de destinació especial[268], la qual només els nodes interessats en la recepció del missatge identificaran com a seva => cal comunicar prèviament quina serà aquesta adreça especial.

        ->exemples: IGMP, AVT, RMT, etc

    - Broadcast – és per a tots els nodes.

        -> s'adreça a l'adreça especial[269], la qual tots els nodes coneixen i la identifiquen com a seva.

        -> exemples: molts dels protocols d'enrutament (DVMRP, etc.), ARP, DHCP, etc.

- Estratègies de comunicació / característiques dels protocols
    - Negociació -> necessitat o no d'establir preacords abans d'iniciar la conversa
        - Connectionless / Stateless
            - no se sap si hi ha el receptor
            - no se sap si el receptor està disponible per a escoltar
            - els paquets només contenen l'adreça de l'emissor i la

267 Aquesta tecnologia no es va implementar fins a la meitat dels anys noranta perquè fins aleshores es pensava que les comunicacions unicast cobrien totes les necessitats; l'aparició de la necessitat de transmetre cadenes d'àudio i de vídeo va fer canviar aquesta percepció inicial.

268 En el protocol IP s'utilitzen les adreces del que havia estat el grup Multicast (224.0.0.0 – 239.255.255.255)

269 Coneguda com a broadcast address.

del receptor sense necessitat de més informació => Stateless perquè ni l'emissor ni el receptor tenen forma de “recordar” si estan en conversa[270]

- datagrama: la unitat de transmissió
- permet la implementació de multicast i broadcast
- els paquets són difícils de filtrar en un firewall

- Connection-oriented[271] / Stateful
  - establiment de connexió -> abans d'iniciar la comunicació hi ha la necessitat, per part de l'emissor, d'informar-ne als receptors
  - apart de les adreces d'origen i de destí, hi ha un identificador de connexió[272] => Stateful perquè tant l'emissor com el receptor poden saber si estan en una conversa o no
  - segment: la unitat de transmissió
  - de naturalesa unicast
  - permet la preconfiguració de l'enrutament[273]

- Fiabilitat -> permet saber a l'emissor si el receptor ha rebut el missatge o no
  - Unreliable
  - Reliable
- detecció d'errors
- correcció d'errors

- Dominis
  - Collision domains

270A nivell de protocol, no de contingut de les dades transmeses.
271És una tècnica molt utilitzada per al control del tràfic IP (MPLS), a on l'increment d'eficiència s'ha traduït en la posposició de la introducció d'altres mecanismes que s'havien postulat imminentment necessaris i que són molt més costosos.
272Per exemple de 10 bits per a Frame Relay, i de 24 bits per a ATM, (ambdós unreliable).
273Un cop enrutats els primers paquets, l'enrutament es pot cachejar, fet que estalvia la necessitat de processar l'algorisme d'enrutament per cada paquet posterior.

        - àrea lògica a on els paquets poden topar entre ells
        - l'eficiència de la xarxa és inversament proporcional al nombre de col·lisions
    - Broadcast domains
        - àrea lògica a on qualsevol node pot parlar amb qualsevol altre sense necessitat d'enrutament
        - àrea lògica a on són audibles els missatges broadcast => quan un node parla, tots els altres escolten per comprovar si el missatge és per a ells.

- Maquinari, segons les capes en què opera cada dispositiu:
    - hub -
        - operen exclusivament sobre la capa OSI 1 – collision domain
        - la velocitat de transmissió de cada node és inversament proporcional al nombre de node connectats
        - cada paquet és escoltat per tots els nodes => carències de seguretat
    - switch -
        - operen sobre la capa OSI 2, a nivell de MAC; es parla de dispositius intel·ligents
        - s'estableixen connexions virtuals entre els nodes creant taules d'assignació entre els seus ports i les MAC dels nodes
        - tots els nodes han de pertànyer a la mateixa xarxa lògica perquè **no** operen a nivell d'IP => no poden parlar a través de xarxes
        - segmenten els collision domains
        - propaguen les peticions broadcast
    - router -
        - operen a la capa OSI 3, a nivell d'IP
        - creen taules d'assignació entre els seus ports i les IPs i les MACs

        - connecten xarxes lògiques diferents
        - segmenten els broadcast domains => no propaguen les peticions broadcast entre xarxes[274]
    - gateway -
        - un router que connecta xarxes físicament diferents => són traductors de protocols

Capa física

- Cablejat, nivells de tensió/intensitat, targes de xarxa, etc.
- Habitualment l'administrador de xarxes quan treballa en aquesta capa es limita a seguir les especificacions dels estàndards[275] per executar els seus projectes.

Capa MAC[276]

- “És a on viuen” els drivers de les targes de xarxa.
- “És la responable” de generar els paquets i de transmetre'ls a través de la capa física.

Adreça MAC

- És l'identificador universal unívoc de les targes de xarxa[277].
- Formada per sis octets, en el sistema EUI-48:
    - Els tres primers identifiquen l'organització que ha emès l'identificador[278].

274 Per exemple, i si no s'especifica el contrari, filtraran les peticions DHCP entre dues xarxes, i per tant, per defecte, un servidor DHCP no sentirà les peticions de qualsevol client que estigui fora de la seva xarxa. Una solució pot ser muntar el servidor DHCP al node que fa de router perquè senti les peticions de qualsevol de les xarxes a què pertany el router.

275 Això no significa que l'administrador de xarxes es pugui desinhibir de conèixer les tecnologies d'aquesta capa, ja que la seva tasca és la d'oferir solucions globals als problemes telemàtics, i per tant, aquestes també exigeixen competències en aquesta capa.

276 Acrònim de Media Access Control.

277 De tecnologies com Ethernet, 802.11 o Bluetooth, entre d'altres (EUI-48) i Firewire i IPv6 (EUI-64).

278 Normalment el fabricant de la tarja.

    - Els tres últims els assigna l'emissor de l'identificador segons el seu criteri.
- Tot i que habitualment les MACs estan gravades físicament als dispositius, en algunes situacions determinades pot ser interessant modificar-la[279] a l'SO:
    - quan un servei es dóna només a una MAC determinada[280].
    - per problemes de llicències sobre unes MAC en concret.
    - Etc.
    - exemple: `# ifconfig eth0 hw ether XX:XX:XX:XX:XX:XX`

Address Protocol Resolution (ARP)

- Protocol d'accés a xarxa que estableix la correspondència entre MAC i adreces IP.
- Cada node té una taula de correspondències.
- La taula de correspondència es pot construir dinàmicament (el més habitual) o estàticament.
- A la taula ARP hi pot haver entrades de cadascun dels nodes veïns dels broadcast domains als que pertanyi el node de la taula.

Exemple: conversa a nivell de MACs per saber a quin node correspon una IP

El node 1 té assignada l'IP 192.168.99.35
El node 2 té assignada l'IP 192.168.99.254 a l'eth0 i la 192.168.99.254 a l'eth2
Pertanyen al mateix broadcast domain
Al node 2 s'hi posa un sniffer[281]
El node 1 llança un ping[282] a l'IP del node 2
Al node 2 es llegeix:

```
[root@node2] # tcpdump -ennqti eth0 \( arp or icmp \)
tcpdump: listening on eth0
0:80:c8:f8:4a:51 ff:ff:ff:ff:ff:ff 42: arp who-has 192.168.99.254 tell 192.168.99.35
0:80:c8:f8:5c:73 0:80:c8:f8:4a:51 60: arp reply 192.168.99.254 is-at 0:80:c8:f8:5c:73
```

279 Aquesta tècnica es coneix com a spoofing.
280 Alguns ISP utilitzen aquesta estratègia per intentar garantir que els usuaris no utilitzin altres dispositius (per exemple routers) dels que ells tenen registrats (normalment NICs).
281 Probablement el més conegut és tcpdump. A Debian forma part del paquet tcpdump. L'aplicació tcptrace (del paquet tcptrace) ajuda a l'anàlisi de les dades capturades amb aquet sniffer.
282 La comanda ping determina si un node es accessible enviant-li una petició de resposta, i esperant la recepció d'aquesta resposta; explota les propietats del protocol ICMP. A Debian forma part del paquet iputils-ping.

```
0:80:c8:f8:4a:51 0:80:c8:f8:5c:73 98: 192.168.99.35 > 192.168.99.254: icmp: echo request
(DF)
0:80:c8:f8:5c:73 0:80:c8:f8:4a:51 98: 192.168.99.254 > 192.168.99.35: icmp: echo reply
```

1era línia-. El node 1 ha llençat una petició ARP broadcast (FF:FF:FF:FF:FF:FF) comunicant la seva MAC (0:80:c8:f8:4a:51) i l'IP associada a aquesta MAC (192.168.99.35) i demanant a quina MAC correspon l'IP 192.168.99.254.

2ona línia-. El node 2 contesta associant a l'IP 192.168.99.254 la MAC de la seva eth0 0:80:c8:f8:5c:73.

3era línia-. El node 1 té prou informació per encapsular paquets ICMP[283] per a realitzar la petició ping.

4rta línia-. El node 2 contesta a la petició ping.

Exemple: comprovació de l'assignació d'una IP a algun node

En la mateixa situació el node 1 pregunta si l'IP 192.168.99.147 pertany algú:

```
[root@node2]# tcpdump -eqtnni eth2 arp
tcpdump: listening on eth2
0:80:c8:f8:4a:51 ff:ff:ff:ff:ff:ff 60: arp who-has 192.168.99.147 (ff:ff:ff:ff:ff:ff)
tell 0.0.0.0
0:80:c8:e8:1e:fc 0:80:c8:f8:4a:51 42: arp reply 192.168.99.147 is-at 0:80:c8:e8:1e:fc
(0:80:c8:e8:1e:fc)

[root@node1]# arping -D -I eth0 192.168.99.147; echo $?
ARPING 192.168.99.147 from 0.0.0.0 eth0
Unicast reply from 192.168.99.147 [00:80:C8:E8:1E:FC] for 192.168.99.147
[00:80:C8:E8:1E:FC] 0.702ms
Sent 1 probes (1 broadcast(s))
Received 1 response(s)
1
```

Consulta a la cache de l'ARP de node 1:

```
[root@node1]# arp -na
? (192.168.99.147) at 00:80:C8:E8:1E:FC [ether] on eth0
? (192.168.99.254) at 00:80:C8:F8:5C:73 [ether] on eth0

[root@node2]# ip neighbor show
192.168.99.147 dev eth0 lladdr 00:80:c8:e8:1e:fc nud reachable
192.168.99.254 dev eth0 lladdr 00:80:c8:f8:5c:73 nud reachable
```

Filtratge ARP

es fa per netfilter/iptables => ja es veurà més endavant

283Aquest protocol presenta característiques tan de la capa d'Internet com de la de transport.

Capa de xarxa o d'IP o d'Internet

- El protocol més utilitzat és l'IP.
- Permet que la convivència de diferents broadcast domains[284] => cal que hi hagi enrutament[285]
- És un protocol unreliable => no es pot saber si un paquet s'ha rebut o no

Adreça IPv4[286], 32bits (quatre octets)

- És l'identificador unívoc d'un node dins d'una xarxa
- L'esquema CIDR[287] fa que l'identificador de xarxa sigui dinàmic[288]:
  - Els n primers bits de l'esquerra serveixen per identificar a la xarxa a la que pertany el node identificat amb la resta de bits (els de la dreta)

    adreça IP
    xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
    n bits de xarxa | 32-n bits de node

  - La màscara de xarxa[289], quatre octets, serveix per determinar quins bits són de xarxa i quins de node:
    - màscaraXarxa AND[290] IP => identificador de xarxa
    - màscaraXarxa NAND IP => identificador de node
  - La parella IP – màscara de xarxa s'acostuma a escriure:
    - especificant la IP i la màscara completa, o
    - IP/número d'uns que té la màscara de xarxa

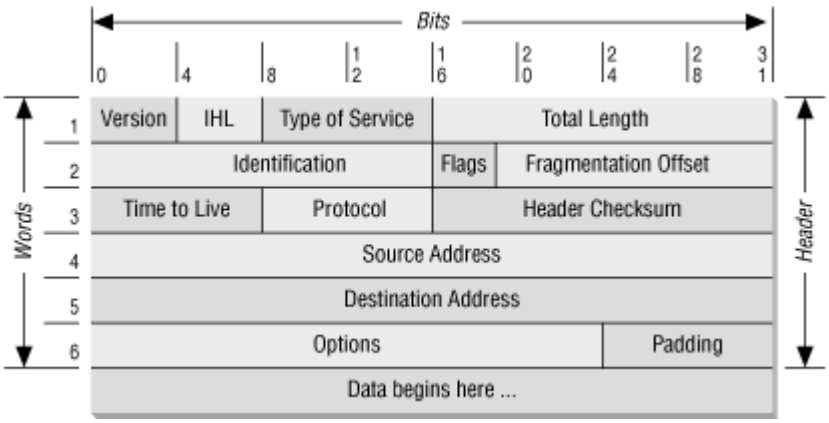
284Això fa que puguin existir xarxes de xarxes.
285Gestionar correctament l'enrutament és una de les tasques complexes a què han de fer front els administradors de xarxes.
286IETF RFC 791 (1981).
287Implantat al 1993.
288Originalment era el primer octet, pel que el nombre de xarxes estava limitat a 256.
289Per a la xarxa local cal que la màscara de xarxa de la interfície de xarxa coincideixi amb la màscara de xarxa de les entrades a la taula d'enrutament de la interfície de xarxa.
290L'aplicació ipcalc, del paquet de Debian ipcalc, està pensada per a automatizar aquests càlculs.

- Permet la creació de subxarxes.

- Adreces reservades més importants[291]:
  - Localhost: 127.0.0.0/8
  - Xarxes privades[292]:

Nom	***Xarxa***	***Bloc CIDR més llarg***	***Quantitat d'IPs***
Bloc de 24bits	10.0.0.0 – 10.255.255.255	10.0.0.0/8	16.777.215
Bloc de 20bits	172.16.0.0 – 172.31.255.255	172.16.0.0/12	1.048.576
Bloc de 16bits	192.168.0.0 – 192.168.255.255	192.168.0.0/16	65.535

  - Xarxes: blocs d'IPs
    - La primera IP d'una xarxa fa referència a la pròpia xarxa
    - L'última IP d'una xarxa és el broadcast de la xarxa[293]



Font: TPC/IP Networking Administration, Craig Hunt. O'Reilly.

Capçalera IPv4

Ipv6[294], 128 bits

291Una llista completa es pot trobar a http://en.wikipedia.org/wiki/IPv4#Allocation.
292Aquestes IPs no són accessibles des d'Internet.
L'administrador pot utilitzar-les indiscriminadament.
293L'adreça de broadcast s'obté fent: adreça de xarxa OR (complament a 1 de la màscara de xarxa).
294A la wikipèdia (http://en.wikipedia.org/wiki/IPv6) hi ha un resum de les tècniques i avantatges que comporta l'IPv6.

- L'IPv6 es proposa per evitar el que es preveu el que serà imminent: l'exhauriment d'adreces Ipv4
- La realitat és que l'ús de subxarxes ha evitat, de moment, el col·lapse de l'IPv4.
- La migració la migració es preveu costosa, difícil i llarga

Configuració d'interfícies de xarxa en Debian /etc/network/interfaces[295]

- Cada secció comença amb una de les tres directrius següents:
  - iface[296]-. va seguida dels tres arguments següents:
    - nom del dispositiu a configurar (eth0)
    - família d'adreça de xarxa:
      - inet-. Per al sistema d'adreces IPv4
      - inet6-. Per al sistema d'adreces IPv6
      - ipx-. Per al sistema d'adreces IPX
    - mètode de configuració:
      - loopback
      - dhcp
      - static ()
      - etc[297].
  - auto-. seguida del nom d'una interfície serveix per especificar que aquesta es configurarà durant el procés d'inicialització[298] i quan es passi el paràmetre -a a qualsevol de les comandes ifupdown.
  - mapping-. mapeja les assignacions per a permetre deferents configuracions de paràmetres en funció de la sortida d'un script.
- A sota de la primera línia de secció es defineixen paràmetres, accions, etc.:
  - up||down líniaDeComandesDeShellAExectutar quan s'afegeix o s'extreu la interfície al sistema

295 `man 5 interfaces`

296 Aquesta serveix per a establir paràmetres de dispositius lògics de xarxa; el conjunt de dispositius lògics d'un dispositiu físic servirà per a determinar la configuració d'aquest dispositiu físic. man ifupdown(8).

297 Els mètodes disponibles estan en funció de la família d'adreces de xarxa.

298 /etc/rcS.d/S40networking.

- per al mètode estàtic:
  - address 192.168.0.1
  - netmask 255.255.248.0
  - gateway[299] 172.19.16.1
  - etc[300].
- per a wifi[301]:
  - wireless-essid NOMWLAN
  - wireless-mode Ad-Hoc
  - wireless-enc restricted
  - wireless-key s:paraula
- etc.

- El pas de paràmetres finalitza quan hi ha una nova línia d'entrada
- Exemple:

```
$ grep -v ´^#´ /etc/network/interfaces
auto lo eth0 eth1

iface lo inet loopback

mapping eth0
      script /usr/local/sbin/get-net-method.sh
      map DYNAMIC eth0-dhcp
      map STATIC eth0-static

iface eth0-dhcp inet dhcp

iface eth0-static inet static
      address 172.19.23.14
      netmask 255.255.248.0
      gateway 172.19.16.1

iface eth1 inet static
      address 192.168.0.1
      netmask 255.255.255.0
      up ip addr add 192.168.0.11/24 dev $IFACE[302]
```

Amb l'/etc/network/interfaces anterior es pot executar, per exemple la comanda:

```
# ifup eth0=eth0-static
```

299Només es pot especificar un gateway dins del fitxer, que serà el que s'utilitzarà per defecte. La resta de gateways caldrà configurar-los manualment (mitjançant un script).

300dns-nameservers

301man 8 iwconfig

302Hooks d'interfície: $IFACE val start o stop segons si s'ha invocat ifup o ifdown, $IFACE conté el nom de la interfície de xarxa, per exemple eth0, $ADDFAM val inet, inet6 o ipx segons la família d'adreces de xarxa i $METHOD identifica el mètode de configuració: static, dhcp, loopback, etc.

Comandes per a la gestió i configuració d'interfície de xarxa		
Paquet	**Comanda**	
iproute[303]	ip[304]	Comanda per excel·lència per a l'administració de xarxes amb Linux.
ifupdown	ifup	Per engegar interfícies de xarxa
	ifdown	Per aturar interfícies de xarxa
wireless-tools	iwconfig	Per assignar valors als paràmetres dels dispositius wireless caractrístics d'aquests

Enrutament

- Es fa node a node
- Cada node IP ha de saber distingir com a mínim entre tres tipus de destinacions (accessibilitat):
  - per a ell mateix => locally hosted addresses[305]
  - localment connectat => locally connected network segment
  - a un altre lloc => necessitat d'enrutament[306]
- Estratègies per a establir l'enrutament:
  - L'enrutament es fa en funció de la destinació final del paquet => una sola taula d'enrutament: ip route
  - L'enrutament es pot prioritzar en funció d'altres característiques del paquet que s'ha d'enrutar => enrutament avançat: ip rule
    - és característic de Linux
    - es defineix més d'una taula d'enrutament
    - les regles de la Routing Policy Database (RPDB) estableixen com s'aniran avaluant les diferents taules d'enrutament

303Aquest paquet conté el document ip-cerf.ps, el qual pot ser molt útil per aprendre com s'utilitza la comanda ip i per aprendre'n a explotar les seves capacitats.
304Aquesta comanda és característica de Linux, ja que explota perfectament les propietats de xarxa d'aquest tipus de nuclis; en d'altres sistemes UNIX cal recórrer a l'ús de diverses comandes per aconseguir configuracions similars. Generalment aquestes comandes també es troben disponibles en Linux: ifconfig, route, arp, etc.
305Com a mínim existeix el loopback, ja que UNIX és un sistema operatiu orientat a xarxa.
306El router ha de ser accessible a nivell de MAC.

Comandes per al seguiment de les rutes dels paquets		
Paquet	**Comanda**	
iputils-tracepath	traceroute	Ruta dels paquets
traceproto	traceproto	Extensió de traceroute que suporta TCP, UDP i ICMP

Taula d'enrutament

- Cada node en té una[307] (com a mínim).
- Estableix a quina interfície de xarxa s'entrega cada paquet.
- Formes de construir la taula d'enrutament:
  - estàticament
    - Es construeix manualment (ip route add).
    - És la que s'utilitza quan només hi ha un únic camí al destí
  - dinàmicament
    - Es construeix de manera transparent a partir de la informació intercanviada pels protocols d'enrutament.
    - És la que s'utilitza quan hi ha més d'un camí possible al destí
    - Avantatges:
      - Resposta dinàmicament a canvis de condicions de les xarxes.
      - Solució més ràpida a problemes complexos d'enrutament.
      - Tria de la solució òptima.
      - Si un paquet no es pot enrutar per un camí, es proba de fer-ho per un d'alternatiu
- exemple:

307En realitat són dues com a mínim: la main, que és a la que es fa referència la majoria de les vegades i que és a la que fa referència la comanda `ip route` per defecte, i la local, que la manté el kernel, i a la qual no s'hi pot afegir entrades manualment. La comanda `ip rule show` mostra les taules que hi ha al sistem.

```
# route
    Kernel IP routing table
    Destination   Gateway        Genmask       Flags Metric Ref Use Iface
    127.0.0.0     *              255.0.0.0     U     0      0     2 lo
    192.168.50.0  *              255.255.255.0 U     0      0   137 eth0
    172.20.0.0    192.168.50.1   255.255.0.0   UG    1      0     7 eth0
    default       192.168.50.254 0.0.0.0       UG    1      0    36 eth0
```

Línia 1a-. tot el tràfic per a la xarxa 127.x.x.x[308] s'envia a lo[309]

Línia 2a-. tot el tràfic per als nodes de la LAN s'envia a eth0

Línia 3a-. tot el tràfic per a la xarxa 172.20.x.x s'envia a eth0 perquè el GW 192.168.50.1 l'enruti adequadament

Línia 4a-. tot el tràfic que no s'hagi enrutat fins ara és per a Internet a on s'hi accedeix pel GW 192.168.50.254

L'* indica que el node destí està a la mateixa xarxa => no s'ha de passar per cap GW

Routing cache

- S'hi emmagatzemen les entrades d'enrutament recents
- El kernel, quan s'ha d'enrutar un paquet:
    - 1er – busca una entrada a la cache per aquella destinació
    - si no la troba, avalua la taula d'enrutament per resoldre l'enrutament

      => quan s'està manipulant/comprovant la taula d'enrutament sempre cal estar al cas dels continguts de la cache d'enrutament.

      `ip route flush cache` -> esborra els continguts de la cache

Capa de transport

- TCP
    - reliable -> s'utilitza el mecanisme PAR:

      l'emissor envia un frame que conté el checksum

308La xarxa 127.x.x.x està reservada per a tasques de loopback.

309La interfície lo (loopback) fa coincidir el canal d'entrada amb el de sortida d'un mateix node. Això permet, entre d'altres coses, que els clients es puguin connectar als servidors que estan a la mateixa màquina.

el receptor rep el frame i en comprova el checksum:

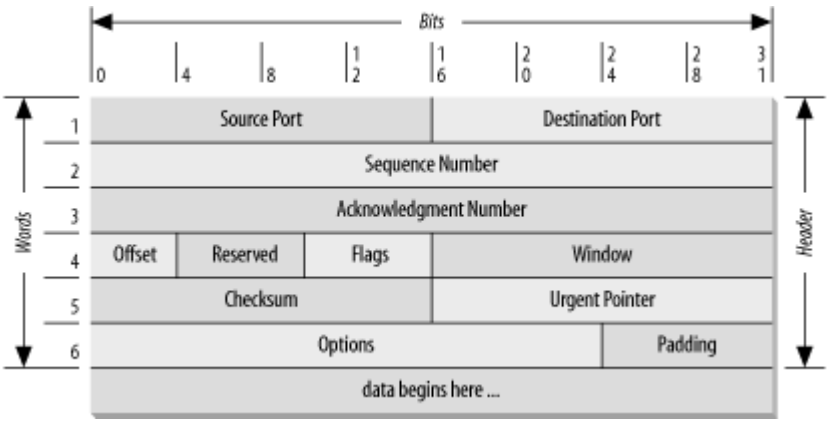
si el checksum és correcte => envia un acknowledgment positiu

sinó descarta el frame[310]

l'emissor espera la rebuda de l'acknowledgment

si al cap d'un temps no l'ha rebut, torna a enviar el frame

- connection-oriented -> three-way handshake[311]
- 8-bit byte-stream -> les dades es veuen com un stream continu => el mateix protocol és responsable del reensamblatge de segments
- unicast

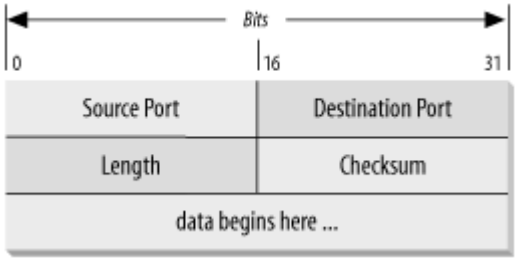


Font: TPC/IP Networking Administration, Craig Hunt. O'Reilly.

Capçalera TCP

- UDP
  - unreliable
  - unicast / multicast

310Tot i que sovint, tant a la literatura, com als fitxers de configuració es parla d'stream
311Perquè en el procés de handshaking s'intercanvien fins a tres segments.



Font: TPC/IP Networking Administration, Craig Hunt. O'Reilly.

Capçalera UDP

Ports i serveis

- La tècnica de la multiplexació permet de serveis a sobre d'una sola connexió física.
- L'IP utilitza els *nombres de protocol* (/etc/protocols) per identificar els protocols de transport.
- Els protocols de transport[312] utilitzen els nombres de port (/etc/services) per identificar les aplicacions.

Rang de ports	***Descripció***
1-1024	Ports privilegiats[313]
1025-49151	Ports registrats[314]
49152-65535	Ports privats[315]

Comandes		
Paquet	**Comanda**	
nmap	nmap	Rastrejament de ports
	nc	llegeix i escriu dades a través d'una connexió de xarxa[316]
	tc	Trafic control

312 Cada protocol de transport té la seva assignació de ports a /etc/services. Així doncs a aquest arxiu s'hi pot torbar `echo 7/tcp` i `echo 7/udp`.
313 Aquestes assignacions són estàndard i són per a serveis ben coneguts.
314 Tot i que oficialment (a través de la IANA) no hi hagi una assignació per aquest rang de ports, sí que es manté un registre (per part de la mateixa IANA) d'assignacions.
315 Els ports d'aquest rang estan disponibles per a fer-ne qualsevol ús.
316 És una eina extremadament útil per als administradors de xarxes; la seva mateixa man page la descriu com la navalla suïssa del TCP/IP.

Filtratge de paquets

- Filtratge estàtic: conjunt de regles a les que es sotmeten tots els paquets
- Filtratge dinàmic: es fa el seguiment de les connexions establertes a través del firewall -> connection tracking

Firewall: netfilter–iptables

netfilter -> sistema de filtratge de paquets compilat dins del kernel.

- Opera entre la capa d'Internet i la de transport => No filtra continguts!!
- proveeix hooks dins de la pila IP els quals poden ser utilitzats per als mòduls per a realitzar operacions sobre els paquets d'acord amb les regles que tinguin a les seves llistes de regles
- mòduls: ip_tables, apr_tables, ip_nat_ftp, ip_conntrack_ftp, etc.

Iptables[317]

- es divideixen en:
  - mòduls del kernel (es distribueixen dins de les fonts del kernel)
    [Networking Options]
    [Network Packet Filtering]
  - eines d'entorn d'usuari[318]:

    /sbin/iptables -> editar les regles dels mòduls

    /sbin/iptables-restore -> per a actualitzar les taules del kernel a partir de fitxer[319]

    /sbin/iptables-save -> per a guardar les taules del kernel a un fitxer

- Funcionament general:
  - Segons la procedencia o destí dels paquets quederan afectats per alguna/es chains (llista de regles).

317En Debian, ambdós paquets, el netfilter i l'iptables, formen part de la instal·lació bàsica.
318A Debian estan dins del paquet iptables.
319Fa més senzill la gestió de les regles.

- Cada regla serveix per dir: “si la capçalera del paquet compleix aquesta *condició*, llavors aplica aquesta chain (target) al paquet”. Sinó es compleix la regla, avalua el compliment de la regla següent de la chain

- Si per un paquet s'arriba al final d'una chain sense que s'hagi complert cap regla, s'aplicarà la built-in target que estableixi la chain policy (-P)

- **Taules**:

  - filter[320] -> taula per defecte (a la que es fa referència si no se n'especifica cap amb -t)

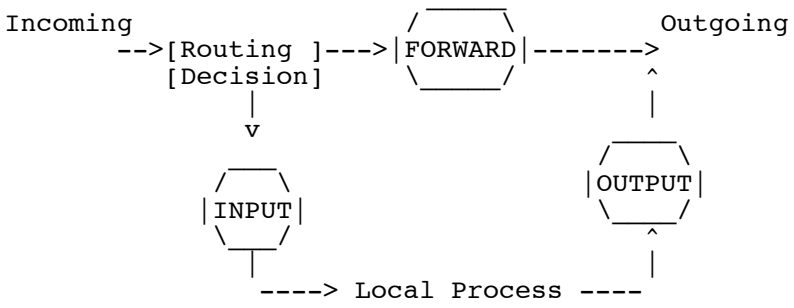
    - buit-in **chains**:

      - INPUT -> fa referència a les capçaleres dels paquets que tenen com a destinació el node local

      - OUTPUT -> fa referència a les capçaleres dels paquets que surten del node local

      - FORWARD -> fa referència a les capçaleres dels paquets que passen pel node local, però que tenen una altra destinació (enrutament)

    - esquema de funcionament:



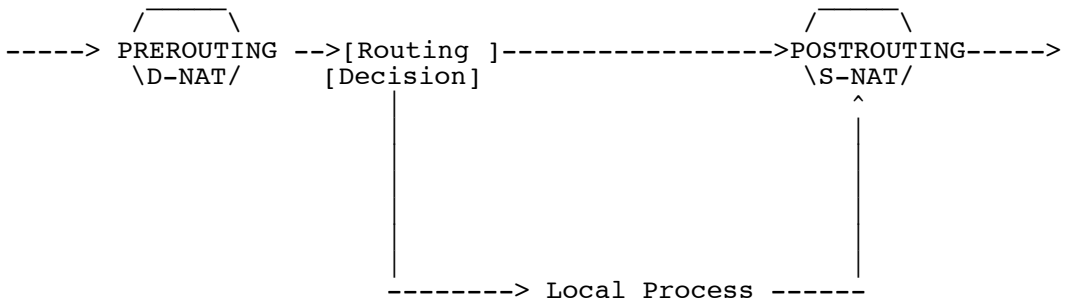
  - nat -> es consulta quan un paquet crea una nova connexió

    -> per a la modificació dels continguts de les capçaleres

    - buit-in chains:

320 És l'única que està carregada al Kernel per defecte. Les altres dues es carreguen tan bon punt se'ls fa menció.

        - PREROUTING -> per alterar les capçaleres tan bon punt arriben
        - OUTPUT -> per alterar les capçaleres dels paquets generats localment abans que s'enrutin
        - POSTROUTING -> per alterar les capçaleres dels paquets just abans que surtin
    - esquema de funcionament:



- mangle -> d'ús exclusiu per a l'alteració especialitzada de capçaleres
    - buit-in chains:
        - PREROUTING -> per alterar les capçaleres dels paquets entrants abans de l'enrutament
        - OUTPUT -> per alterar les capçaleres dels paquets generats localment abans que s'enrutin
        - INPUT -> per alterar les capçaleres dels paquets que tenen per destinació el mateix node
        - FORWARD -> per alterar les capçaleres dels paquets que passen pel node, però que no són per al node
        - POSTROUTING -> per alterar les capçaleres dels paquets just abans que surtin

- Targets
    - chain definida per l'usuari -> al final acabarà essent una de les altres
    - ACCEPT -> es deixa passar el paquet, quedant lliure de la chain predecessora

- DROP -> s'elimina el paquet
- QUEUE -> el paquet es passa a l'user-space (si ho suporta el kernel)
- RETURN -> para d'aplicar la chain que el conté i es continua aplicant les regles de la chain predecessora

- Target Extensions -> es carreguen modularment de forma automàtica
    - LOG -> (non-terminating target => si es vol fer alguna altra cosa amb el paquet cal especificar-ho a la chain següent amb la mateix matching criteria)
    - REJECT -> igual que DROP, però es retorna un paquet d'error a l'emissor
    - SNAT -> taula nat, chain PREROUTING. Opcions:
      --to-source ipaddr[ipaddr][:port]
    - DNAT -> taula nat, chain PREROUTING. Opcions:
      --to-destinatio ipaddr[ipaddr][:port]
    - MASQUERADE, REDIRECT, etc.

- Opcions

  -t, --table table -> per especificar la taula; filter per defecte

  - Comandes -> accions a fer amb les regles

    -A, --apend chain rule-specification

    -D, --delete chain rule-specification|rulenum

    -L, --list [chain] -> llista en conjunt de regles

      -L -v -> verbose
      -L -Z -> llista i reseteja els comptadors

    -h, --help

  - Paràmetres -> constitueixen una especificació d'una regla

    -p, --protocol [!] protocol

-s, --source, --src [!] address[/mask]

-d, --destination, --dst [!] address[/mask]

-j, --jump target -> indica la chain que se li aplicacrà

- Altres opcions -> opcions que es poden afegir

  -v, --verbose

  -n, --numeric -> IP i ports en format numèric

- Match extensios -> l'ús de --protocol o de --match (-m) seguit del nom-del-mòdul força la càrrega de mòduls que afegeixen opcions per a construir regles:

Nom del mòdul	***Opcions afegides***
tcp	--source-port [!] port[:port]
	--destination-port [!] port[:port]
	--syn -> només ho compleixen els paquets amb el SYN bit a u i els ACK i FIN a zero
udp	--source-port [!] port[:port]
	--destination-port [!] port[:port]
mac	--mac-source [!] address
conntrack -> permet fer el seguiment de les conneccions	-- cstate state a on state és una llista separada per comes d'alguns dels elements següents: INVALID -> per a paquets dels quals no se'n coneix cap comunicació associada ESTABLISHED -> per als paquets que tenen associada una connexió NEW-> per a obrir l'associació d'una connexió RELATED -> per a establir una nova associació per a una connexió que ja és coneguda
etc.	

- Exemple: Política a seguir per defecte: denegar tot allò que no estigui explícitament permès, en el cas de l'exemple lo i connexions SSH a adreces locals vàlides; les peticions broadcast i multicast es poden

habilitar o deshabilitar:

```
#/etc/network/iptables
*filter
:INPUT DROP [0:0]
:FORWARD DROP  [0:0]
:OUTPUT ACCEPT  [0:0]

#a new chain:
:drop-not-to-me - [0:0]

#allow localhost traffic
-A INPUT -i lo -j ACCEPT

#drop-not-to-me associated to INPUT
-A INPUT -j drop-not-to-me

#drop everything not inteded for me
-A drop-not-to-me -m addrtype --dst-type LOCAL -j RETURN
#-A drop-not-to-me -m addrtype --dst-type BROADCAST -j RETURN
#-A drop-not-to-me -m addrtype --dst-type MULTICAST -j RETURN
-A drop-not-to-me -j DROP

#accept packets of established connections (stateful)
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT


#drop invalid packets, or non-SYN packets of unknown connections
-A INPUT -m conntrack --ctstate INVALID -j DROP

#accept incoming SSH connections
-A INPUT -p tcp --dport ssh -j ACCEPT

COMMIT

<<EOF>>
```

per actualitzar les taules al kernel:

```
# iptables-restore < /etc/network/iptables
```

per a guardar a un fitxer les taules del kernel actuals:

```
# iptables-save > fitxer
```

IPMasquerading o NAT

- A Linux és un cas especial d'ús de Netfilter
- Permet l'accés d'una xarxa amb IPs privades a Internet.
- Cal reescriure les capçaleres dels paquets. És transparent a l'usuari.
- Hi ha diverses tècniques => cal triar la més convenient en cada cas.

- Hi ha protocols que necessiten helpers per funcionar[321] sobre NAT (les peticions DCC sortints sobre IRC, per exemple).

Anàlisi del tràfic de xarxa: Ethereal

- Programa per les X molt potent i útil
- Entre d'altres prestacions, permet analitzar les captures realitzades amb tcpdump

Capa d'aplicació

- formes de donar servei:
  - daemon -> /etc/init.d/* i runlevels
    - un procés, normalment en background, s'escolta un port específic de forma permanentment
    - un cop es detecta una petició al port:
      - el mateix procés pot atendre la petició
      - alternativament es pot generar un procés fill que atengui la petició, per un port no estàndard, i el pare pot continuar esperant més peticions pel port estàndard.
  - inetd o xinited -> Internet daemon
    - el superdaemon escolta diversos ports (els configurats)
      - quan hi ha una petició a un port que està escoltant “desperta” el procés que haurà d'atendre la petició

SNMP

Open SSH – connexions d'encriptació asimètrica[322] entre nodes

321 Això és degut que part de la negociació client-servidor es fa dins de les dades dels paquets.

322 Estrictament parlant l'encriptació asimètrica només s'utilitza a l'inici de la connexió durant l'establiment de claus i la negociació de les primeres claus simètriques. A partir d'aquest moment ja s'utilitzen les claus simètriques negociades per a la comunicació. La

- Paquets:
  - openssh-client
    - ssh -> per a l'establiment de connexions
    - scp -> substitució de l'rcp
    - sftp -> client per a l'sftp-server
    - ssh-agent -> per a la gestió de claus durant
    - ssh-add -> per afegir claus a gestionar per ssh-agent
    - ssh-keygen -> per a generar parelles de claus
    - ssh-keyscan -> per recollir claus públiques
  - openssh-server
    - sshd -> servidor ssh[323]
    - sftp-server -> servidor d'ftp per ssh
- Fitxers
  - personals ~/.ssh/
    - id_rsa -> clau privada
    - id_rsa.pub -> clau pública[324]
    - authorized_keys -> col·lecció de claus públiques reconegudes
    - know_hosts -> col·lecció de claus públiques de servidors reconeguts
  - de servidor /etc/hosts/ssh/
    - id_host_rsa_key -> clau privada del servidor
    - id_host_rsa_key.pub -> clau pública del servidor
- Passphrase
  - És un mètode per a protegir la clau pública
  - Problema per als processos desatesos ja que sempre s'hauria d'entrar manualment[325]

---

rotació de claus utilitzades dificulta l'obtenció de les claus per a d'intercepció de la comunicació. Cal tenir present que la codificació asimètrica és molt més costosa computacionalment parlant que no pas la simètrica.
Aquest tipus de codificacions tenen el seu fonament teòric en les funcions hash i en la impossibilitat de descompondre computacionalment de manera eficient enters grans.

323 Tot i que no s'utilitzin els mecanismes d'intercanvi de claus personals, es recomana sempre utilitzar aquest client-servidor per a establir connexions de sessió, ja que aquestes es fan sempre per un canal segur.

324 Aquesta és la que cal propagar (posar dins del fitxer authorized_keys) a totes les destinacions a on voldrem realitzar connexions segures.

325 Si es deixa en un arxiu, es pot robar, com passa amb la clau pública.

Resolució de noms

- La taula de nodes (/etc/hosts) és una solució parcial del problema de la resolució de noms.
- DNS
  - solució als problemes essencials de la taula de nodes:
    - no es depèn d'una sola taula (té bona escalabilitat)
    - es garanteix la propagació (per tant no hi ha d'haver una autoritat central per gestionar dominis)
  - solució client-servidor:
    - El client, o resolver, és un conjunt de rutines[326] que es presenten a la resta d'aplicacions que necessiten el servei de resolució en forma de llibreria[327].
    - servidors:
      - authoritive server-. servidor que té la informació sobre el node per el que s'està preguntant.
      - local server-. servidor que passa les peticions i les cacheja[328].
  - estructura jeràrquica distribuïda:
    - root domain-. Centralitza l'estructura piramidal però no conté informació sobre la resolució, que es delga als TLD.
    - root servers o top-level domains (TLD)
      - code country TLD (ccTLD): .uk, .fr, .de, etc.
      - generic TLD o general-purpose TLD (gTLD): .com, .org, etc[329].

326 Que saben a qui s'ha de preguntar, i com s'ha de preguntar, davant d'una petició de resolució.

327 Els sistemes que només integren la part client del sistema DNS es coneixen com a sistemes resolver-only; aquesta és la configuració més habitual per a sistemes d'escriptori.

328 D'aquesta manera es crea una base de dades locals de resolució que evita haver de passar peticions futures.

329 Inicialment l'organisme rector de l'associació de noms, la Internet Corporation for Assigned Names and Numbers (ICANN), només reconeixa els set dominis següents per als gTLD: .com, .edu, .gov, .mil, .net, .int i .org. Donat el col·lapse que pateixen aquests

- La implementació de DNS en els sistemes UNIX és el BIND(v9):
    - named-. daemon de la part servidora. Té tres modes d'operació:
        - Master[330]-. Conté tota la informació d'un domini sobre el qual té autoritat[331].
        - Slave[332]-. Conté una rèplica actualitzada[333] de les bases de dades del master/s.
        - Caching-only-. Obtenen totes les respostes de la resta de servidors i les cachegen per poder respondre la propera vegada que se'ls demani la resolució

Correu

- Sobre TCP
- Basat en text
- MUA -> interfícies d'usuari
- MTA -> Servidors responsables del repartiment del correu
- SPAM -> un dels grans problemes

- ESMTP
    - Estàndard de facto del repartiment de correu (relay) a Internet
    - substitut/extensió de SMTP -> es distingeixen per la paraula clau d'inici de transmissió:

        HELO -> SMTP
        EHLO -> ESMTP

    - MIME -> imatges, àudio, vídeo, audio, aplicacions, etc.
    - SMTP-AUTH-> imposa l'obligació d'identificar-se per a poder fer relay

---

dominis, i en especial el .com, l'any 2000 l'ICANN va augmentar en nombre de dominis amb els següents: .aero, .biz, .coop, .museum, .pro, .info i .name.

330 També són coneguts com a servidors primaris.

331 És a dir, que ell té tota la informació sobre els dominis que gestiona i que sempre respondrà acuradament. Només hi hauria d'haver un màster per cada domini.

332 També són coneguts com a servidors secundaris.

333 L'actualització es fa de forma periòdica.

```
$ telnet localhost 25
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 macosx.powerbook.ct ESMTP Postfix
quit
221 Bye
Connection closed by foreign host.
```

- POP -> per a baixar el correu des del servidor (SMTP) al node local, a on es processarà amb un MUA

```
$ telnet localhost 110
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
+OK <a4ff42383a26e95af86591f61b2cb4c1@getaway.local>
user nil0
+OK Tell me your password.
pass nil0233
+OK Welcome aboard! You have no messages at all.
quit
+OK Done
Connection closed by foreign host.
```

- IMAP -> permet la baixada de correu com el POP, amb propietats afegides
    - possibilita la manipulació individual de missatges remotament
    - sincronització de mailboxes remota/local
    - té més comandes que POP

6è Capítol: Apache

Conceptes previs

Negociació de continguts-. La pàgina que serveix el servidor està en funció d'alguna preferència del navegador del client (idiomàtica, per exemple).

Apache 1.3, 2.0, i 2.2

- Apache 1.3
  - Ben coneguda => aplicacions crítiques
  - Ben testejada => poques releases => es poden utilitzar els binaris directament
  - Model de procés prefork[334]:
    - processos múltiples
    - pre-fork
    - no threads
    - cada procés controla una sola petició simultàniament.
  - La que va representar l'explosió d'Apache
- Apache 2.0
  - Releases freqüents pròpies d'un projecte en desenvolupament => cal anar a les fonts i s'ha d'estar al cas
  - Es pot triar el model de procés: MPM[335]s
    - winnt

334Un procés de control pare llança n fills que queden a l'escolta de possibles peticions. Quan es produeix una petició un procés fill l'atén i el procés de control pare crea un altre procés fill que es posa a escoltar. Així sempre hi ha n fills escoltant i quan es produeix la petició no cal esperar que es crei el procés que l'atendrà.
Amb la comanda ps aux, per exemple, es pot comprovar l'existència d'aquests n fills i el pare quan encara no s'està donant cap servei.

335Acrònim de multiprocessing modules.

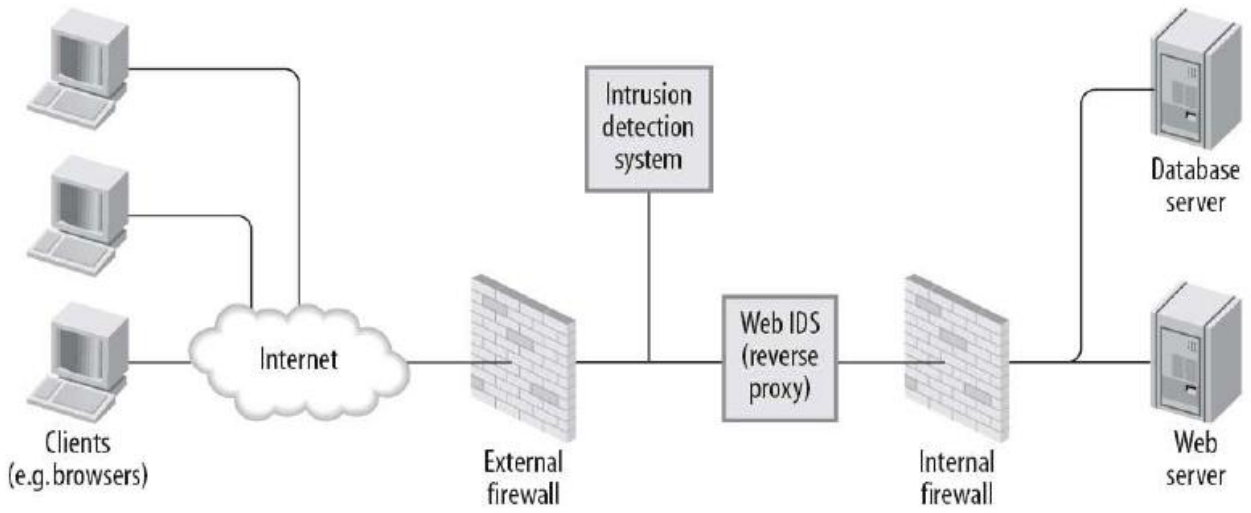
        - un únic procés[336]
        - múltiples threads d'execució
        - utilitza les eines natives de xarxa de MS
        - concebut per a MS Windows[337]
    - prefork
        - tecnologia similar a la de l'Apache 1.3
        - és el que garanteix més robustesa, ja que les peticions s'atenen de forma aïllada
        - per a sistemes UNIX
    - worker
        - híbrid entre multiprocés i mutithread
        - treu més rendiment al maquinari
        - pensat per a l'escalabilitat
        - Per a sistemes UNIX
- Apache 2.2
    - creació recent
    - es pretén que sigui el substitut de Apache 1.3[338]
    - des del projecte es demana que s'utilitzi aquesta versió per agilitzar les taques de depuració
    - Afegeix l'MPM event
        - derivat del worker
        - pensat per a l'alta escalabilitat

336Un únic procés de control que llança un sol procés fill, el qual, mitjançant la creació de threads, atén a les peticions.
Un error en l'atenció d'una petició pot comprometre tot el sistema.

337En aquesta plataforma la implementació de la tecnologia prefork dóna molt mals resultats ja que el sistema operatiu té dificultats a l'hora de gestionar alguns processos a l'hora.

338La realitat mostra que la migració de la versió 1.3 a la 2.0 no ha estat total ni molt menys. Molts administradors, encara avui, es decanten per a la solució 1.3, la qual ha donat proves més que suficients de la seva “solvència”.

- atén més peticions simultàniament[339]



Font: Apache security, Ivan Ristic. O'Reilly.

Configuració per augmentar la seguretat.

Proxy SQUID

Instal·lació i configuració bàsica des de les fonts

Descàrrega del codi font i compilació

1. A l'adreça http://www.apache.org/ se'ns indicarà quin mirror ens pot anar bé, per exemple apache.gva.es:

   ```
   $ wget http://apache.gva.es/httpd/apache[340]_x.yy.zz[341].tar.gz
   ```

2. Integritat de les fonts

   - MD5: les dues comandes han de mostrar el mateix resultat per pantalla:

     ```
     $ md5sum apache_x.yy.zz.tar.gz

     $wget -0 - -q \
     http://www.apache.org/dist/httpd/apache_x.yy.zz.tar.gz.mda
     ```

   - GPG: utilitzant criptografia de clau pública:

339 Les peticions les escolten uns threads, i les atenen uns altres, de manera que els primers poden tornar a la tasca d'escoltar.
340 A la versió 2 és `httpd`.
341 Cal substituir x pel número de versió (1.3, 2.0 o 2.2) i el número de release.

```
$ wget http://apache.gva.es/httpd/apache_x.yy.zz.tar.gz.asc
```

`$ gpg apache_x.yy.zz.tar.gz.asc` -> indica quin ID s'ha d'utilitzar per obtenir la clau del servidor de claus:

`$ gpg –keyserver pgpkeys.mit.edu –recv-key ID`[342] -> mostra si la clau és vàlida o no

3. Compilació:

   `$ ./configure –help` -> mostra la llista de mòduls, i si es compilaran o no

   ```
   $ ./configure \
   --prefix=/usr/local/apache \
   ```
   -> indica a on s'instalaran els binaris

   `--enable-rewrite`[343] `\` -> per afegir mòduls que estan exclosos a la llista

   `--disable-imap`[344] `\` -> per treure mòduls que s'haurien de compliar

   ```
   $ make

   # make install
   ```

4. Llistat de mòduls compilats:

   ```
   $ ./apache -l
   ```

httpd.conf mínim

/usr/local/apache/conf/httpd.conf:

```
ServerRoot /usr/local/apache

DocumentRoot /var/www/htdocs

PidFile /var/www/logs/apache.pid

Listen 80

HostNameLookup off
```

Usuari i grup per a l'execució d'apache

Per defecte apache s'executa com a nobody. És molt més segur que cada servei s'executi amb el seu usuari exclusiu (departamentalització):

```
# groupadd http
```

342Cal substituir ID de clau obtingut a la comanda anterior.
343Per a les versions 2: `--enable-module=rewrite` .
344Per a les versions 2: `--disable-module=imap` .

```
# useradd httpd -g httpd -d /dev/null -s /sbin/nologin
```

/usr/local/apache/conf/httpd.conf:

```
User httpd
Group httpd
```

Permisos dels fitxers

```
# chown -R root:root /usr/local/apache
# find /usr/local/apache -type d | xargs chmod 755
# find /usr/local/apache -type f | xargs chmod 644
```

`# chmod -R go-r /usr/local/apache/conf` -> per accedir-hi: sudo

`# chmod -R go-r /usr/local/apache/logs` -> per accedir-hi: sudo

Instal·lació i configuració bàsica amb els binaris de Debian

-> la gran majoria dels passos anteriors es fan de forma automàtica quan l'apache s'instal·la des dels repositoris de Debian. Si no hi ha cap motiu que justifiqui la seva compliació des del codi font, sempre és més segur utilitzar la versió precompilada.

- # apt-get install apache -> versió 1.3.34
- httpd.conf: `/etc/apache/httpd.conf`
- usuari: www-data
- grup: www-data
- logs: /var/log/

Configuracions bàsiques de seguretat

Directoris a servir per defecte

Si no s'especifica el contrari apache serveix qualsevol fitxer que li sigui accessible => un error de configuració es pot traduir en l'exposició accidental d'informació vital per al sistema.

=> es denega per defecte l'accés a qualsevol directori, i després s'especifica quins es poden servir, /var/www/htdocs:

httpd.conf:

```
<Directory />
      Order Deny, Allow
      Deny from all
      Options[345] None
      AllowOverride None
</Directory>
<Directory /var/www/htdocs>
      Order Allow,Deny
      Allow from all
</Directory>
```

Directriu `Options`

Dins de la directriu `<Directory>`, pot tenir un o més valors dels següents:

`Options`	
Valor	**Comentari**
`All`	Totes les opcions següents excepte `None` i `MultiViews` **=> MOLTA ATENCIÓ als problemes de seguretat!!!!**
`None`	No s'habilita cap de les opcions restants
`ExecCGI`	Permet l'execució d'scripts CGI
`FollowSymLinks`*	Permet el seguiment de symlinks[346] a l'hora de servir.
`Includes`	Permet includes per la banda del servidor
`IncludesNOEXEC`	Permet SSIs però no la comada `exec`. No afecte als CGIs
`Indexes`	Permet que el servidor serveixi la llista d'arxius del directori quan no hi ha un arxiu index
`MultiViews`	Permet la negociació de continguts
`SymLinksIfOwnerMatch`	Només servirà els symlinks sii el propietari dels simlinks i dels destins és el matix

* Alternativament als symlinks es pot utilitzar la directriu `Alias`:també serveix per incorporar un directori a l'arbre a servir, i es fa d'una manera més segura

Exemple: `Options -FollowSymLinks +SymLinksIfOwnerMatch`

345Si no es vol utilitzar la negociació de continguts és recomanable deshabilitar totes les opcions d'`Options` per evitar forats de seguretat.

346Si un usuari del sistema crea symlinks que apuntin fora dels directoris i no s'especifica res més, el servidor servirà els continguts sobre els que apunten els symlinks; per tant és recomanable que en comptes d'aquesta opció s'utilitzi l'opció SymLinksIfOwnerMatch.

Directriu `AllowOverride`

Per defecte apache permet que als directoris a servir hi hagi dades de configuració (.htaccess) les quals poden sobreescriure la configuració provinent del fitxer principal (httpd.conf). Això, apart de fer baixar el rendiment del servidor, ja que a cada directori ha de comprovar si hi ha dades de configuració a tenir en compte, fa que qualsevol usuari pugui modificar la configuració del servidor

Dins de la directriu `<Directory>`, pot tenir un o més valors dels següents:

`AllowOverride`	
`AuthConfig`	Permet l'ús de directrius d'autorització
`FileInfo`	Permet l'ús de directrius per controlar els tipus de document
`Indexes`	Permet l'ús de directrius per controlar l'indexat del directori
`Limit`	Permet l'ús de directrius per controlar l'accés al host
`Options`	Permet l'ús de directrius per controlar funcions específiques de directori[347]
`All`	Habilita totes les opcions anteriors
`None`	Ignora els .htacces

Escripts CGI

Per raons de seguretat els scripts convé tenir-los en directoris aïllats per poder-los controlar i monotoritzar:

- es pot fer utilitzant la directriu `Options`:

```
<Directory /var/www/cgi-bin>
     Options ExecCGI
     SetHandler cgi-script
</Directory>
```

- Alternativament es pot utilitzar la directiu `ScriptAlias` que crea un directori virtual nou; cal per tant utilitzar la directriu `<Directory>` per establir els permisos del directori real[348].

Logging

- Access log

347 Per exemple la inclusió d'`Options` a `AllowOverride` permet que s'utilitzin, fent-ne cas, directrius de configuració de PHP a `.htaccess`

348 Excepcionalment si els dos directoris, el real i l'alies, es diuen igual no caldria.

```
LogFormat "%h %l %u \" %>s %b \" %{User-Agent}i\"" combined
CustomLog /var/www/logs/access_log combined
```

- Error log

```
LogLevel info
ErrorLog /var/www/logs/error_log
```

Límits al servidor

Directriu	***Valor suggerit***	***Comentaris***
`TimeOut`	60	El valor per defecte, 300, segons, és massa alt davant de DoS
`KeepAlive`	On	
`MaxKeepAliveRequests`	100	
`KeepAliveTimeout`	15	
`LimitRequestBody`	64000	Limit HTML
`LimitRequestFields`	100	Limit HTML
`LimitRequestFieldsize`	8190	Limit HTML
`LimitXMLRequestBody`[349]	1000000	Limit HTML
`MinSpareServers`	5	
`MaxSpareServers`	10	
`StartServers`	5	
`MaxClients`	150	
`MaxRequestsPerChild`	1000	A l'Apache 1.3 té valor 0 per defecte.

Gàbies chroot

- Confinament:
  - Sense shell
  - Sense accés a eines de compilació

349És específica d'Apache 2 i s'utilitza en el mòdul mod_dav.

    - Sense binaris suid

- Tipus
    - External chroot -> primer es crea la gàbia. Més segur.
    - Internal chroot -> la gàbia es crea un cop s'ha inicialitzat el procés

Internal chroot

- La forma habitual de fer-ho és utilitzant els mòduls següents:
    - mod_security http://www.modsecurity.org

      ```
      SecChrootDir /chroot/apache
      ```

    - mod_chroot http://core.segfault.pl/~hobbit/mod_chroot/

      ```
      ChrootDir /chroot/apache
      ```

- Limitacions:
    - Només es pot utilitzar Apache i els seus mòduls.
    - Durant l'execució del servidor no s'inicialitzen processos => els CGIs s'han de compilar estàticament.
    - Durant l'execució no es pot accedir a fitxers externs a la gàbia.

External chroot

- bash engabiat: un exemple senzill

  ```
  #mkdir /chroot
  ```

  ```
  #chroot /chroot /bin/bash
  chroot: /bin/bash: No such file or directory
  ```
  -> falla pq a dins de la gàbia no hi ha res

  ```
  #mkdir /chroot/bin
  ```

  ```
  #cp /bin/bash /chroot/bin/bash
  ```

  #chroot /chroot /bin/bash
  ```
  chroot: /bin/bash: No such file or directory
  ```
  -> falla per dependències:

  ```
  # ldd /bin/bash
        libtermcap.so.2 => /lib/libtermcap.so.2 (0x0088a000)
  ```

```
        libdl.so.2 => /lib/libdl.so.2 (0x0060b000)
        libc.so.6 => /lib/tls/libc.so.6 (0x004ac000)
        /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x00494000)

# mkdir /chroot/lib

#cp /lib/libtermcap.so.2 /lib/libdl.so.e /lib/libc.so.6 \
/lib/ld-linux.so.2 /chroot/lib

#chroot /chroot /bin/bash
bash-2.05b#
```

-> ara només es poden utilitzar comandes built-in:

```
bash-2.05b# echo /lib/*
/lib/ld-linux.so.2 /lib/libc.so.6 /lib/libdl.so.2
/lib/libtermcap.so.2
```

- Apache a la gàbia

```
# mkdir -p /chroot/apache/usr/local
# mv /usr/local/apache /chroot/apache/usr/local
# ln -s /chroot/apache/usr/local/apache /usr/local/apache
# mkdir -p /chroot/apache/var
# mv /var/www /chroot/apache/var/
# ln -s /chroot/apache/var/www /var/www
# ldd /chroot/apache/usr/local/apache/bin/httpd
        libm.so.6 => /lib/tls/libm.so.6 (0x005e7000)
        libcrypt.so.1 => /lib/libcrypt.so.1 (0x00623000)
        libgdbm.so.2 => /usr/lib/libgdbm.so.2 (0x00902000)
        libexpat.so.0 => /usr/lib/libexpat.so.0 (0x00930000)
        libdl.so.2 => /lib/libdl.so.2 (0x0060b000)
        libc.so.6 => /lib/tls/libc.so.6 (0x004ac000)
        /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x00494000)
# mkdir /chroot/apache/lib
# cp /lib/tls/libm.so.6 /lib/libcrypt.so.1 /usr/lib/libgdbm.so.2 \
/usr/lib/libexpat.so.0 /lib/libdl.so.2 /lib/tls/libc.so.6 \
/lib/ld-linux.so.2 /chroot/apache/lib
```

-> sistema d'autentificació:

```
# mkdir /chroot/apache/etc
# cp /etc/nsswitch.conf /chroot/apache/etc/
# cp /lib/libnss_files.so.2 /chroot/apache/lib
```

-> usuari i grup

```
# echo "httpd:x:500:500:Apache:/:/sbin/nologin" > \
/chroot/apache/etc/passwd
# echo "httpd:x:500:" > /chroot/apache/etc/group
```

-> resolució de noms

```
# cp /lib/libnss_dns.so.2 /chroot/apache/lib
# cp /etc/hosts /chroot/apache/etc
# cp /etc/resolv.conf /chroot/apache/etc
```

-> /dev/ necessaris

```
# mkdir /chroot/apache/dev
# mknod -m 666 /chroot/apache/dev/null c 1 3
# mknod -m 666 /chroot/apache/dev/zero c 1 5
```

```
# mknod -m 644 /chroot/apache/dev/random c 1 8
```

-> directori temporal

```
# mkdir /chroot/apache/tmp
# chmod +t /chroot/apache/tmp
# chmod 777 /chroot/apache/tmp
```

-> configuració horària

```
# cp /usr/share/zoneinfo/MET /chroot/apache/etc/localtime
```

-> locales

```
# mkdir -p /chroot/apache/usr/lib/locale
# set | grep LANG
LANG=en_US
LANGVAR=en_US
# cp -dpR /usr/lib/locale/en_US /chroot/apache/usr/lib/locale
```

- **PHP a la gàbia**

- **Perl a la gàbia**

- **MySQL a la gàbia**

Control d'accés

- Conceptes
  - **Identificació**-. Procés en el qual l'usuari presenta la seva identitat
  - **Autentificació**-. Procés en el qual es verifica si l'usuari té accés al sistema
  - **Autorització**-. Procés en el qual es verifica si l'usuari té accés a un recurs determinat
  - **Registre** (accountability)-. Procés de registre de qui ha accedit a quins recursos, quan ho ha fet i com ho ha fet

Autentificació

- És el que cal fer sempre abans de servir qualsevol altra cosa per raons de seguretat
- Tormes de fer-ho:
  - utilitzant eines del protocol HTTP:
    - Autentificació bàsica:
      - Problemes:
        - Les credencials viatgen en text pla
        - S'han de passar a cada petició ja que el servidor no té mecanismes des sessió[350]
        - No hi ha mecanismes explícits per a fer log out (es fa automàticament al final de cada petició o per timeout)
        - El login no es pot personalitzar
      - Funcionament: per credencials en text pla
        - El client ha d'afegir a la petició una línia Authorization; sinó ho fa rep un missatge d'error indicant-li que el reialme necessita autentificació
    - Autentificació digest
      - Problemes:
        - L'atacant pot extreure recursos de la comunicació ja que viatge en text pla
        - Tot i que l'atacant no pugui robar el password si que pot utilitzar el càlcul de la funció resultant (replay attack[351])
      - Funcionament: l'objectiu és no utilitzar credencials en clar
        - El servidor envia un missatge al client

350Perquè l'HTTP és un protocol stateless.

351El password és capturat per una tercera persona que espera que el servidor tanqui la connexió original per timeout, i llavors utilitza la informació capturada per a obrir una nova sessió.

- El client computa el valor de la funció hash del missatge del servidor i del password

- transferint el problema a l'aplicació:
  - Autentificació basada en formulari
    - Avantatges:
      - No hi intervé el servidor web => no cal que els programadors d'aplicacions hi tinguin accés
      - S'utilitzen eines externes al servidor web tan per a validar passwords com per emmagatzemar-los
      - Com que la gestió es fa fora del protocol HTTP es poden implementar mecanismes de sessió[352]

=> ús d'SSL/TLS està plenament justificat

Public Key Infraestructure

- Estratègies que hi conflueixen:
  - Encriptació de clau assimètrica
  - Certificats digitals
  - Autoritats Certificadores

- Certificats digitals
  - S'utilitzen:

    per identificar-se

    i per signar documents[353]
  - Els pot emetre:
    - Un individu => poca confiança
    - Entitats certificadores privades => es poden utilitzar internament

352Per tant, només caldrà validar-se una vegada.
353El que fan les autoritats certificadores és signar una clau digitat amb el que es coneix com root certificate.

        - Entitats certificadores públiques => es poden utilitzar públicament

- Xarxes de confiança (webs of trust)
    - Els usuaris d'una xarxa, per constituir-la, es signen entre ells[354], un a un, els certificats
    - És una alternativa a la necessitat de les CA

354Basant-se en una trobada física: en un coneixement mutu.

7è Capítol: MySQL

Introducció

Base de dades (Database, DB): Col·lecció **organitzada** de dades.

Base de dades relacional (Relational DB, RDB): DB organitzada segons el **model relacional**[355].

Standard Query Language (SQL): És un llenguatge per a la manipulació del contingut de les RDB.

Relational Database Management System (RDBMS): Entorn de treball basat en SQL.

En un RDBMS hi pot haver més d'una **base de dades**, cada una de les quals està formada per una o més **taules**. Una taula és un conjunt dades disposades matricialment: cada columna, **camp** (field), representa una propietat, i cada fila és una **entrada** (record) a la taula. Una taula sempre tindrà un nombre determinat de camps.

Eines RDBMS de P. Ll. típiques[356]:

MySQL-. Una de les més conegudes. Senzilla d'utilitzar. Companya natural de PHP per a DB amb front-end web.

PostgreSQL-. Probablement la més sofisticada i potent. És solució per a entorns empresarials de producció.

Base-. GUI molt intuïtiva que posa a l'abast de tothom un RDBMS. Forma part del paquet OpenOffice v.2.

MySQL

- Atenció la llicència MySQL -> si hi ha ànim de lucre té conseqüències econòmiques
- Pot manegar BD força grans

Arquitectura

355 http://en.wikipedia.org/wiki/Relational_model
356 Fora del PL altres RDBMS coneguts són Oracle i Microsoft Access

- El procés mysqld interactua amb les bases de dades i atén les peticions dels clients
- Els clients poden establir connexió amb el servidor per:
  - Sockets-. Si servidor i client estan al mateix node

    + ràpid

    -> s'utilitza per defecte o si el host (-h) és localhost
  - Xarxa-. Utilitzant connexions TCP/IP

    -> s'ha de configurar a my.cnf[357]

Instal·lació i configuració

- A Debian es divideix en dos paquets: mysql-server i mysql-client

1. El primer que cal fer després de la instal·lació és establir el password de l'usuari[358] root, ja que per defecte aquest no té password

```
$ mysqladmin -u root password 'el_password'
```

2. Creem una base de dades

```
$ mysql -u root -p

mysql> CREAT DATABASE bd_lamp;
```

3. Creem un usuari regular i li assignem privilegis sobre la bd_lamp

```
mysql> GRANT SELECT, INSERT, UPDATE, DELETE bd_lamp.* TO
'lamp' IDENTIFIED BY 'lamppass';
```

4. Fem efectius els canvis

```
mysql> FLUSH PRIVILEGES;
```

PRIVILEGI	***Acció***
SELECT	Llegeix files de les taules
INSERT	Afegeix files de dades a les taules
UPDATE	Actualitza dades de les taules
DELETE	Borra dades de les taules

357A Debian /etc/mysql/my.cnf.
358Els usuaris de la base de dades i els usuaris de sistema no tenen res a veure.

PRIVILEGI	***Acció***
INDEX	Crea i elimina index de les taules
ALTER	Modifica l'estructura d'una base de dades
CREATE	Crea taules noves d'una base de dades
DROP	Elimina taules o bases de dades
RELOAD	Rellegeix l'assignació de taules (i per tant actualitza els canvis d'usuaris)
SHUTDOWN	Para el mysqld
PROCESS	Atura el mysqld
FILE	Adquisició de dades des de fitxers de text
GRANT	Crea nous usuaris i els assigna permisos
REVOKE	Elimina permisos als usuaris

Exemple senzill d'ús

1. Plantejament:

   Es vol crear una base de dades amb una sola taula que contingui els usuaris d'un sistema i certa informació addicional de cada un d'ells:

Taula usuaris	
Camp	Exemple
id_usuari	834
nom	Pau
cognom	Ble
email	Pau.ble@cinc.cat
password	paupass
data_registre	2006-3-31 17:04:02

2. Tipus

   Es classifiquen en:

   - Text
   - Nombres
   - Dates i hores

   Una primera aproximació:

Taula usuaris	
Camp	Tipus
id_usuari	nombre
nom	text
cognom	text
email	text
password	text
data_registre	data / hora

3. Alguns tipus

Tipus	***Espai***	***Descripció***
CHAR[longitud]	longitud	Camp de longitud fixe de 0 a 255 caràcters de llarg
VARCHAR[longitud]	longitud + 1 byte	Camp de longitud variable de 0 a 255 caràcters de llarg
MEDIUMINT	3 bytes	Enter d'entre -2^-24 i 2^24
DATE	3 bytes	HH:MM:SS
DATETIME	8 bytes	YYYY-MM-DD HH:MM:SS

CHAR -> de longitud fixe
-> d'accés ràpid
VARCHAR
-> de longitud variable => optimització de l'espai
-> d'accés lent[359]

Taula usuaris	
Camp	Exemple
id_usuari	MEDIUMINT
nom	VARCHAR(15)
cognom	VARCHAR(30)
email	VARCHAR(40)
password	VARCHAR(40)
data_registre	DATETIME

359No si s'utilitzen taules InnoDB.

4. Altres propietats dels camps

Propietat	***Descripció***
NULL	Que no té valor
NO NULL	Que no es pot deixar sense valor
UNSIGNED	Que no pot prendre valors negatius
ZEROFILL[360]	Els espais vuits s'omplen amb 0
AUTO_INCREMENT	

Taula usuaris	
Camp	Exemple
id_usuari	MEDIUMINT UNSIGNED NOT NULL
nom	VARCHAR(15) NOT NULL
cognom	VARCHAR(30) NOT NULL
email	VARCHAR(40) NOT NULL
password	VARCHAR(40) NOT NULL
data_registre	DATETIME NOT NULL

5. Creació de la taula usuaris

```
$ mysql -u root -password -p -h localhost

mysql> CREAT DATABASE proves;

mysql> GRANT ALL proves.* TO 'usuari' IDENTIFIED BY 'passusuari';

mysql> exit

$ mysql -u usuari -p

mysql> SHOW DATABASES;

+------------+
| Database   |
+------------+
| db_lamp    |
| mysql      |
| proves     |
| test       |
+------------+

4 rows in set (0.00 sec)

mysql> USE proves;
```

360Són automàticament UNSIGNED.

```
mysql> CREATE TABLE usuaris (
    -> id_usuari MEDIUMINT UNSIGNED NOT NULL AUTO_INCREMENT,
    -> nom VARCHAR(15) NOT NULL,
    -> cognom CARCHAR(30) NOT NULL,
    -> email VARCHAR(40) NOT NULL,
    -> password CHAR(40) NOT NULL,
    -> data_registre DATETIME NOT NULL,
    -> PRIMARY KEY (id_usuari)
    -> );

mysql> SHOW TABLES;

+------------------+
| Tables_in_proves |
+------------------+
| usuaris          |
+------------------+

mysql> SHOW COLUMNS FROM usuaris;
+---------------+----------------------+------+-----+---------------------+----------------+
| Field         | Type                 | Null | Key | Default             | Extra          |
+---------------+----------------------+------+-----+---------------------+----------------+
| id_usuari     | mediumint(8) unsigned |      | PRI | NULL                | auto_increment|
| nom           | varchar(15)          |      |     |                     |                |
| cognom        | varchar(30)          |      |     |                     |                |
| email         | varchar(40)          |      |     |                     |                |
| password      | varchar(40)          |      |     |                     |                |
| data_registre | datetime             |      |     | 0000-00-00 00:00:00 |                |
+---------------+----------------------+------+-----+---------------------+----------------+

mysql> DESCRIBE usuaris;
+---------------+----------------------+------+-----+---------------------+----------------+
| Field         | Type                 | Null | Key | Default             | Extra          |
+---------------+----------------------+------+-----+---------------------+----------------+
| id_usuari     | mediumint(8) unsigned |      | PRI | NULL                | auto_increment|
| nom           | varchar(15)          |      |     |                     |                |
| cognom        | varchar(30)          |      |     |                     |                |
| email         | varchar(40)          |      |     |                     |                |
| password      | varchar(40)          |      |     |                     |                |
| data_registre | datetime             |      |     | 0000-00-00 00:00:00 |                |
+---------------+----------------------+------+-----+---------------------+----------------+
```

Funcions	
SHA()	Funció d'encriptació unidireccional. Retorna un string de **40 caràcters**. Fins a MySQL 4.1 s'utilitzava la funció MD5(), la qual retorna un string de 32 caràcters.
NOW()	Retorna YYYY-MM-DD HH:MM:SS

6. Càrrega de dades a la taula usuaris

   Regles:
   - Els valors **numèrics mai** entre cometes
   - Els valors d'**string sempre** entre comentes
   - Les **dates i hores sempre** entre comentes
   - Les **funcions mai** entre comentes
   - La paraula **NULL mai** entre cometes

- Per línia de comandes:

- INSERT INTO nomtaula (columna1, ...) VALUES ('valor1', ...);

  ->Permet especificar aquells camps que es volen omplir

- INSERT INTO nomtaula VALUES ('valor1', NULL, ..., 'valorn')

  -> Cal especificar **tots** els valors d'una fila

  ```
  mysql> INSERT INTO usuaris VALUES
  (NULL,'Roger','Baig','roger.baig@gmail.com',SHA('roger'),NOW()
  );
  ```

- Des de fitxer de text amb les cel·les separades per tabuladors:

  LOAD DATA LOCAL INFILE '/cami/al/fitxer.txt' INTO TABLE nomtaula

  ```
  mysql> LOAD DATA LOCAL INFILE './db_exemple.txt' INTO TABLE
  usuaris;
  ```

7. Cerques a la taula:

```
mysql> SELECT id_usuari, nom FROM users;

mysql> SELECT id_usuari, nom FROM users LIMIT 3;

mysql> SELECT id_usuari, nom FROM users LIMIT 3,2;[361]

mysql> SELECT nom, id_usuari, nom FROM users ;

mysql> SELECT * FROM users;

mysql> SELECT * FROM users WHERE (id_usuari >= 2) AND (id_usuari
<5);

mysql> SELECT * FROM users WHERE email IS NULL;[362]

mysql> SELECT * FROM users WHERE email='';[363]

mysql> SELECT * FROM users WHERE password=SHA('elpassword');
```

8. Ordenació de cerques

   SELECT nomcolumna1,... FROM nomtaula ORDER BY columna [DESC]

```
mysql> SELECT id_usuari, nom, cognom FROM users ORDER BY cognom;
```

361La clàusula GROUP BY és molt útil a l'hora de paginar llistes de més d'un full.
362Aquí, per complir-se la condició cal que el camp email ha de tenir assignat el valor NULL.
363En aquest cas la condició es complirà si i només si a email no se li ha assignat cap valor; si val NULL ja no es complirà, ja que NULL ja és un valor.

9. Actualització de les dades de la taula

   UPDATE nomtaula SET nomcolumna1='valor',... WHERE nomcolumnax='valor'

   ```
   mysql> UPDATE usuaris SET cognom='Vinas' WHERE nom='roger';
   ```

10. Retirada de dades de la taula

    DELETE FROM nomtalua WHERE nomcolumna='valor' -> esborra entrades a la taula

    DELETE FROM nomtalua -> esborra tots els continguts de la taula mantenint-ne l'estructura

    TRUNCATE TABLE nomtalua -> esborra tots els continguts de la taula i l'estructura; després reescriu l'estructura[364]

    DROP [TABLE nomtaula | DATABASE nomdebasededades] -> elimina taules o bases de dades

364TRUNCATE és molt més segur, a l'hora de destruir dades, que no pas DELETE (utilitzen mètode s diferents).

8è Capítol: PHP

9è Capítol: LAMP

10è Capítol: Taller

Activitats per capítols

Activitats capítol 1: Introducció

1a-. Si teniu experiència en alguna distribució de GNU/Linux o en més d'una digues:

1. Quina és? quin sistema de paquets utilitza?
2. Sota quin tipus de llicència es distribueix el programari que inclou?
3. Quin sistema de paquets utilitza?
4. Utilitzes preferentment el programari empaquetat o prefereixes recompilar-lo tu mateix des dels codi font?
5. Té algun sistema de gestió/instal·lació centralitzat?
6. Quina és la utilitat principal que li dónes?
7. Utilitzes el sistema gràfic?
8. Quins window manager utilitzes? Saps avaluar la quantitat de recursos de maquinari que utilitzen? Quines diferències perceps entre ells?
9. Si coneixes més d'una distribució de GNU/Linux, compara-les entre elles, digues quines diferències hi trobes i en quines ocasions prefereixes una o altra.

Activitats capítol 2n: El Projecte Debian

1a-. Abans de procedir a la instal·lació de qualsevol distribució cal que analitzem detingudament alguns aspectes per avaluar com n'hem de fer la instal·lació. Fes una llista dels aspectes que creguis que s'han de tenir resolts abans d'iniciar una instal·lació, i digues quina solució els hi donaries per al cas que hem de tractar al projecte del màster: muntar un servidor per allotjar un LCMS.

2a-. Feu la instal·lació de GNU/Linux Debian d'acord amb el que heu analitzat a la primera activitat. Tingueu en compte que pot ser les necessitats que voleu cobrir amb aquesta instal·lació no siguin les mateixes que les condicionaran la instal·lació a l'aula. Preneu notes dels passos que considereu més importats i de qualsevol dubte o qüestió que us quedi sense resposta per poder-les analitzar a la sessió següent.

Activitats capítol 3r: Usuari

1a-. Quines diferències hi ha entre les línies de comandes següents? A on rauen aquestes diferències?

```
echo 2 * 3 > 5 és una inigualtat correcta.
echo ´2 * 3 >5 és una inigualtat correcta.´
echo ´2 * 3 > 5´ és una inigualtat correcta.
```

```
echo 2 \* 3 \> 5 és una inigualtat correcta.
```

2a-. Fes les taules de veritat que estimis necessàries per provar que l'exemple que s'ha utilitzat per il·lustrar el funcionament de l'umask és correcte.

3a-. Si la variable CAMI està assgnada a /home/pop/llibre/resultats.fitxer.txt, prediu justificadament què retornaran cada una de les expressions següents:

```
${CAMI##/*/}
${CAMI#/*/}
${CAMI}
${CAMI%.*}
${CAMI%%.*}
```

4a-. Feu un script que passant-li el nom d'un directori com a paràmetre d'entrada assigni a tots els seus subdirectoris els permisos 755 i 644 als fitxers que aquests contenen.

5a-. Expliqueu el perquè la línia de comandes adjunta fa el que fa:

```
$ls /etc/*
```

6a-. Consulteu la man page d'stiky i feu-ne el resum.

Activitats capítol 4t: Administració Local

1a-. Feu un script que faci un tarball comprimit de tot un directori (amb els seus subdirectoris, links, i arxius) i que l'anomeni backup-AA.MM.DD.tar.bz2, a on AA.MM.DD és la data de creació (any, mes i dia). Creeu un archive d'un directori amb l'script que heu creat i desempaqueteu-lo en un altre directori i comproveu que tot està correctament direccionat (especialment els links simbòlics).

2a-. Feu que l'script que heu generat a l'activitat anterior s'executi automàticament cada dia a la mateixa hora. Feu, també de manera automàtica, que un cop s'hagi acabat l'operació de crear el paquet, un usuari anomenat backup copii, mitjançant l'establiment d'una connexió segura, l'arxiu de backup al seu directori home.

3a-. Comproveu que els mecanismes de backup que heu programat a les dues activitats anteriors efectivament funcionen i que és possible substituir el directori original per un backup sense perdre informació.

Activitats capítol 5è: Administració de Xarxa

1a-. Aprofitant el que s'ha fet a les activitats del capítol 4t, feu que una altra màquina copii via scp el backup.

Bibliografia bàsica

Bibliografia Per Capítols

Capítol 1r: Introducció

- Al Web:
  - http://www.gnu.org/gnu/manifesto.html -. The GNU Manifesto. Richard Stallman.
  - <z http://www.gnu.org/copyleft/gpl.html -. The GNU General Public License.
  - http://www.opensource.org/halloween/ -. The Halloween Documents. Eric S. Raymond.
  - http://www.opensource.org/docs/definition.php -.The Open Source Definition.

- En format paper:
  - Just for Fun: The Story of an Accidental Revolutionary. Linus Torvalds, David Diamond. Harper Collins Publishers.
  - Open Sources: Voices from the Open Source Revolution. Chris DiBona, Sam Ockman, Mark Stone. O'Reilly.

Capítol 2n: El Projecte Debian

- Paquets Debian[365]:
  - debian-reference -. Conté el Debian Refernce Manual; recomanat per un cop s'ha acabat la instal·lació i arriba l'hora de personlitzar el sistema i de fer-lo servir (http://qref.sf.net)
  - doc-debian -. Documentació que cal consultar abans de preguntar qualsevol cosa.
  - Harden-doc -. Conté el Securiting Debian Manual; conté tot el que es referix a garantir la seguretat del sistema.
  - apt-howto -. Conté l'apt HOWTO.
  - Debian-policy -. Conté la Debian policy. La seva lectura és recomanable si es vol conèixer una mica el projecte.
  - developers-reference -. Per ampliar coneixements.
  - newbiedoc -. Documentació per a “principiants” de Debian.

- Al Web
  - http://colt.projectgamma.com/hands-on/ -. Hands-on Guide to the

365Per tant s'instal·len com qualsevol altre paquet.

Debian GNU Operating System. Davor Ocelic.
    - http://survivor.sarovar.org -. Debian GNU/Linux Desktop Survival Guide. Graham Williams.
    - http://debian-administration.org -. Lloc de concentració de documentació per als administradors de Debian.

- A l'IRC: xarxa Freenode (irc.debian.org)
    - #debian canal principal
    - #debian-catala canal de Debian en català
    - #debian-es canal de Debian en castellà

- Llistes de correu
    - lists.debian.org

- News
    - http://debianplanet.org -. Per estar al dia del que passa a Debian[366].

- En format paper:
    - The Debian System: Concepts and Technologies. Martin F. Krafft. No Starch Press. United States of America2005.

3r Capítol: Usuari

- Al Web
    - http://www.gnu.org/software/bash/manual/bash.html Bash reference manual. Chet Ramey, Brian Fox.
    - http://www.tldp.org/LDP/abs/ Advanced Bash-Scripting Guide. Mendel Cooper.
    - http://www.unix.org.ua/oreilly Col·lecció completa de O'Reilly “CD Bookshelf”.
    - A http://learnlinux.tsf.org.za/courses/build/sys-admin/ System Administration. Matthew West.

- En format paper
    - Learning the bash. Cameron Newham, Bill Rosenblatt. O'Reilly & Associates,Inc.
    - Learning Perl. Randal L. Schwarts, Tom Phenix, Brian d Foy. O'Reilly.
    - Learning Python. Mark Lutz, David Ascher. O'Reilly.

4t Capítol: Administració Local

- Al Web:

366Tot i que en el moment de la redacció d'aquest text la màquina no dóna servei, s'espera que ho torni ha fer d'aquí a unes quantes setmanes.

- http://www.linuxfromscratch.org/ Pàgina principal del projecte Linux from Scatch.
- http://tldp.org/HOWTO/From-PowerUp-To-Bash-Prompt-HOWTO.html The from powerup to bash prompt HOWTO, Greg Keefe.
- http://tldp.org/HOWTO/LVM-HOWTO/ The LVM HOWTO, Aj Lewis.
- http://tldp.org/HOWTO/Software-RAID-HOWTO.html The Software-RAID HOWTO, Jakob Ostergaard i Emilio Bueso.
- http://www.debian.org/doc/manuals/securing-debian-howto/ Securing Debian Manual

5è Capítol: Administració de Xarxa

- Al Web:
  - http://linux-ip.net/ Guide to IP Layer Networking Administration with Linux. Martin A.Brown.
  - http://www.netfilter.org/documentation/index.html Pàgina de documentació del projecte netfilter.org. Molts HOWTOs (Networking Concepts, Package Filtering, Netfilter Hacking, NAT, etc.) i tutorials interessants.
  - http://qref.sourceforge.net/Debian/reference/reference.en.html Debian Reference

- Fòrum:
  - http://debian-administration.org

6è Capítol: Apache

- Al Web:
  - http://www.gnupg.org/gph/en/manual.html -. The Gnu Privacy Handbook
  - a http://www.cryptnet.net/fdp/crypto/gpg-party.html GnuPG Keysharing Party HOWTO

- En format paper
  -

7è Capítol: MySQL

8è Capítol: PHP

9è Capítol: LAMP

10è Capítol: Taller

Acrònims

Acrònim	***Significat***
ARP	Address Resolution Protocol
Bash	Burn-Again shell
BIND	Berkeley Interenet Name Domain
CIDR	Classless Inter-Domain Routing
DNS	Domain Name Server o System
ESMTP	Extended Simple Mail Transfer Protocol
FTP	File Transfer Protocol
grep	global regular expression and print
HTTP	HyperText Transfer Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IRC	Internet Relay Chat
LSB	Linux Standard Base
MAC	Media Accesss Control
MIME	Multipurpose Internet Mail Extensions
MTA	Mail Transfer Agent
MUA	Mail User Agent
NAT	Network Address Translation
PAR	Positive Acknowledgment with Retransmission
POP	Post Office Protocol
OSI	Open Systems Interconnection
sed	stream editor
SSH	Secure Shell
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol

GNU Free Documentation License

Version 1.2, November 2002

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- **A.** Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- **B.** List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- **C.** State on the Title page the name of the publisher of the Modified Version, as the publisher.
- **D.** Preserve all the copyright notices of the Document.
- **E.** Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- **F.** Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- **G.** Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- **H.** Include an unaltered copy of this License.
- **I.** Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- **J.** Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- **K.** For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- **L.** Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- **M.** Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- **N.** Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- **O.** Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements."

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.