tocol) [dhc93]. Això significa que l'estació es configurarà sola només connectant el cable de xarxa, un cop s'hagin configurat els protocols necessaris. El fet de configurar la xarxa de l'estació de treball mitjançant el protocol DHCP és imprescindible, ja que així es centralitza l'assignació d'adreces IP a tots els components de l'arquitectura des del servidor central. És aquest servidor el que te configurat el protocol DHCP per assignar IPs a tots els components de l'arquitectura Skolelinux, a excepció dels clients lleugers. Els clients lleugers formen part d'una subxarxa separada (figura 5) i les adreces IPs són assignades pel servidor de clients lleugers.

En la resta de components de l'arquitectura, i en el cas que ens centra de les estacions de treball, s'ha de configurar un client DHCP, que és l'encarregat de comunicar-se amb el servidor principal per obtenir l'adreça IP corresponent. Aquesta IP és normalment del rang 10.0.2.0/23 a excepció dels clients lleugers, que tenen assignades IPs del rang 192.168.0.0/24.

En l'algorisme 1 es pot veure el fitxer de configuració de la interfície de xarxa (/etc/sysconfig/network/ifcfg-eth-id-00:10:5A:DE:3E:71). Aquesta configuració s'aplica a l'estació de treball a l'iniciar-se el PC i, sempre i quan, l'estació de treball tingui connectivitat amb el servidor principal, si aquest no està operatiu no pot assignar adreces IP. Així docs, Cal també configurar el protocol dhcp, mitjançant el fitxer dhcp.conf, per poder establir una comunicació entre la workstation i el servidor principal. Això es fa introduïnt l'adreça IP o el nom del servidor principal en el fitxer esmentat anteriorment.

Algorithm 1 Fitxer de configuració de la interfície de xarxa

```
BOOTPROTO='dhcp'
MTU=''
REMOTE_IPADDR=''
STARTMODE='auto'
UNIQUE='vuMS.Er3ucFQoZE2'
USERCONTROL='no'
_nm_name='bus-pci-0000:00:0e.0'
```

Finalment, un cop arrancat el sistema, el resum de les configuracions de

les interfícies de xarxa es pot veure en l'algorisme 2. Aquesta workstation ja forma part de l'arquitectura Skolelinux, almenys a nivell de xarxa.

Algorithm 2 Resum de configuració interficíes de xarxa

eth0 Link encap:Ethernet HWaddr 00:10:5A:DE:3E:71MM
inet addr:10.0.2.237 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::210:5aff:fede:3e71/64 Scope:Link
UP BROADCAST NOTRAILERS MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:25 errors:0 dropped:0 overruns:0 carrier:25
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b) TX bytes:11670 (11.3 Kb)
Interrupt:11 Base address:0x1000

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:148 errors:0 dropped:0 overruns:0 frame:0
TX packets:148 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:9298 (9.0 Kb) TX bytes:9298 (9.0 Kb)

4.3.2 Seguretat en la xarxa

En la xarxa Skolelinux on es realitzen les proves d'integració de l'estació de treball un dels components és un router que dona accés a internet a tots els dispositius interns. Aquest router també te la missió d'exercir de tallafocs de tot el sistema, és per aquesta raó que no se n'hi ha instal·lat cap en l'estació de treball. Aquest sistema és del tipus de protecció perifèrica, que dota d'una certa seguretat a tota la xarxa vers atacs exteriors.

Pel que fa a la protecció interna, de l'estació de treball, el propi sistema operatiu incorpora per defecte d'una pantalla on s'ha d'introduir un nom d'usuari i una contrasenya correctes per poder accedir al sistema. Com que l'estació encara no pot validar usuaris de l'arquitectura, només s'ha permés

l'accés al sistema a l'administrador (root), així doncs sense la contrasenya d'aquest usuari no és pot entrar al sistema.

No s'ha cregut convenient la instal·lació d'un tallafoc local, ja que hauria de permetre l'accés a tots els usuaris del sistema que volguessin accedir als serveis de l'estació i, a l'inversa, tots els usuaris de l'estació haurien de poder accedir als serveis de la xarxa. És a dir, no seria útil perquè hauria de permetre accés a molts, sinó tots, els ports. Un altre component de la seguretat local és el fet de disposar d'un antivirus, s'ha decidit instal·lar-ne un d'accés lliure que te suport per linux, es tracta d'Avast!. Aquest antivirus és d'instal·lació molt ràpida i s'actualitza molt freqüentment i de forma automàtica amb les signatures dels virus més coneguts. És cert que no hi ha molts virus creats per a les plataformes linux però quan més persones facin servir aquest sistema operatiu del segur que apareixen més virus, per tant s'ha optat per prevenir.

4.4 Configuració dels serveis

En aquest punt es pot dir que la primera fase d'integració de l'estació de treball dins l'arquitectura Skolelinux s'ha completat. Es disposa d'una estació de treball amb sistema operatiu GNU/Linux de la distribució OpenSUSE totalment operativa, que a nivell de xarxa forma part d'aquesta arquitectura. Ara és el moment de començar amb la segona fase, configurar els diferents serveis de l'estació, tant aquells serveis que ha d'oferir als altres dispositius de la xarxa Skolelinux com aquells que han d'ésser accessibles des d'un usuari de l'estació de treball.

Tot component que es desitgi incloure dins l'arquitectura Skolelinux ha de tindre una sèrie de serveis configurats, ja sigui una estació de treball o un client lleuger. Aquests serveis són de dos tipus, els genèrics i els específics de cada component. Els serveis genèrics són aquells que tot component de l'arquitectura Skolelinux he de tindre configurat, com ara la sincronització del rellotge amb el servidor principal, l'accés al servidors de noms (DNS) o la configuració de la xarxa mitjançant el protocol DHCP. Per altra banda, els serveis específics són aquells que, depenen del component que els oferta,

seran diferents, per tant els serveis que ofereix una workstation són totalment diferents dels que ofereix un servidor de clients lleugers.

En la taula 2 es pot veure un resum dels serveis que s'han de configurar en l'estació de treball, en els següents punt se'n farà una descripció detallada tant de les funcionalitats de cada servei com de la forma de configurar-los.

Estació de treball	
Serveis genèrics	**Serveis específics**
logging centralitzat	Configuració servei SSHD
Accés al DNS	Configuració copies de seguretat
Configuració per DHCP	Compartició impressores
Accés al servidor de fitxers	Compartició CDs/DVDs
Configuració protocol NTP	
Configuració servidor correu	
Accés al LDAP	
Accés servidor web	
Accés servidor SQL	

Table 2: Serveis d'una estació de treball

L'únic servei que ja s'ha comentat amb anterioritat és la configuració de l'estació de treball per DHCP, detallat en el punt *4.3.1 Configuració de la xarxa.*

4.4.1 Logging centralitzat

Tots els serveis que s'han de configurar en aquesta estació de treball tenen processos associats que són els responsables de publicitar aquell servei a altres components. Tots aquests processos generen informació respecte l'estat del servei, aquesta informació, ja siguin errors o informació de l'estat actual, és emmagatzemada en uns fitxers anomenats popularment "fitxers de logs". Son fitxers de text que van acumulant informació de l'estat de cada servei amb un cert format, encara que aquest format no ha d'ésser igual per a tots els serveis.

Per defecte, cada procés és responsable d'emmagatzemar la informació que cregui necessària en els diferents fitxers de logs. La naturalesa d'aquest fet implica una descentralització, ja que cada procés crearà el seu fitxer de

log dins del PC on està executant-se. Això es per aportar una certa claredat, si cada procés crea un fitxer de logs és molt fàcil localitzar un error d'un determinat servei, en canvi si tots els logs convergissin en un únic fitxer seria molt més difícil trobar la causa de l'error.

L'especificació dels serveis de l'arquitectura Skolelinux, recomana centralitzar tots els fitxers de logs en un sol punt, el servidor centra. Això no vol dir que s'hagin d'unificar tots els fitxers de logs, cada servei tindrà el seu fitxer però localitzat en un altre dispositiu de l'arquitectura. Així doncs, per unificar tots aquests missatges de log, l'arquitectura Skolelinux, estableix que el servidor principal és el responsable d'emmagatzemar tots aquests fitxers i missatges de log. Per tant, cada component de l'arquitectura ha de configurar el procés "syslog"[sys80] per poder enviar tots aquests missatges a través de la xarxa fins el servidor principal.

Per defecte, cap configuració d'un servidor no està predefinida per a que pugui rebre el missatges de log d'altres servidors, cada PC o servidor emmagatzema de forma local els logs creats. No és el cas del servidor principal de Skolelinux, que ja disposa del perfil configurat per rebre i tractar el missatges de log provinents d'altres components de l'arquitectura Skolelinux. Així doncs només cal configurar els clients, en aquest cas l'estació de treball, per a que enviï els missatges de log a través de la xarxa i s'emmagatzemin en el servidor central. A continuació es pot veure la línia que s'ha d'afegir al fitxer /etc/syslog.conf, on tjener.intern és el nom del servidor principal que s'ha donat d'alta al DNS.

```
*.debug          @tjener.intern
```

Un cop modificat el fitxer responsable de la configuració dels logs, només cal reiniciar el servei que està actiu a l'estació de treball i, automàticament, tots els missatges seran enviats al servidor central.

4.4.2 Configuració del DNS

Fins ara s'ha parlat molt del DNS, que fa aquest servei exactament? És realment necessària la seva configuració? A continuació s'intentarà explicar

el perquè de la inclusió d'aquest servei a l'arquitectura Skolelinux i la forma de configurar-lo.

Es pot dir doncs, que el DNS (Domain Name System) [dns83] és el servei encarregat d'associar informació diversa amb el nom d'un servei dins un domini. Un bon símil seria que la seva funció és la mateixa que te una guia de telèfons, en la guia donat un nom es busca el número de telèfon associat, en el DNS donat un nom de servei obtenim l'adreça del component que l'ofereix. A nivell d'internet s'utilitza per traduir els noms dels dominis (www.exemple.cat), utilitzat per a ésser entesos per les persones, a adreces IP (192.168.1.1), que són les utilitzades per les màquines per comunicar-se les unes amb les altres. La conclusió és que el DNS és un servei imprescindible en la utilització d'internet.

Sabent quina és la utilització més comú d'aquest servei a internet, quina és la utilitat d'instal·lar-lo en l'arquitectura Skolelinux doncs? Com s'ha dit, un servidor de DNS tradueix el nom d'un servei a l'adreça IP del component que oferta el determinat servei. Doncs només cal aplicar aquest principi a l'arquitectura Skolelinux. En tota l'arquitectura pot haver-hi només un component que ofereixi el servei de DNS, per defecte és el servidor central, ja que aquest servidor és l'únic component que està present en totes les configuracions de l'arquitectura i el servei és imprescindible que existeixi.

En aquest punt ja se sap quina és la seva funcionalitat i quin servidor ofereix el servei de DNS, ara cal saber quines avantatges ofereix, la principal és la portabilitat del servei. Es pot donar el cas que un servei ofertat inicialment per un component, passi a ésser ofertat per un altre al cap del temps. Això pot ser degut a que el segon servidor te major capacitat de procés i s'estima que el servei funcionarà millor o senzillament perquè s'ha de donar de baixa un determinat component i el servei s'ha de migrar a algun altre lloc. Ja de per sí és prou costosa la migració d'un servei que només faltaria modificar totes les referències a aquell servei en els altres components del sistema, per evitar aquesta situació hi ha el servidor de DNS. Totes les referències a un determinat servei, de tots els components del sistema, no es duen a terme de forma directa sinó a través del DNS, cap component es refereix, per exemple, al servidor de NTP com una adreça IP sinó que jo fa amb el

nom ntp.tjener.intern o ntp.tjener. Així, en el cas que el servidor NTP canviï d'ubicació només caldrà modificar la referència del servidor DNS i els altres components podran accedir-hi igualment sense haver de canviar res.

Sabent doncs que la configuració del DNS és útil a l'hora de buscar u oferir tant un servei com l'ordenador que ofereix el servei, cal configurar tots i cadascun dels serveis publicitats per l'estació de treball en el servidor que te configurat el DNS, per defecte el servidor principal. És a dir, en el servidor principal es donaran d'alta els serveis i el PC que els ofereix, afegint el següent parell ≪IP - Nom del servei≫ o ≪Nom del component - Nom del servei≫ en el DNS. És necessari seguir unes determinades pautes a l'hora de donar d'alta els serveis, com ara:

- Com a nom de servei s'utilitzarà, sempre que sigui possible, el nom del protocol que publicita el servei, com per exemple ldap o ntp.
- En el moment de donar d'alta un servei, en comptes d'introduir la adreça IP directament, s'introdueix el nom donat d'alta al DNS que correspon a l'estació de treball.
- Només hi haurà tuples del tipus $<<$IP - Nom$>>$ en la definició dels noms dels components que formen l'arquitectura Skolelinux, mai en la definició dels serveis.

4.4.3 Sincronització del rellotge

La sincronització del rellotge es realitza mitjançant el protocol NTP [ntp84], aquest protocol treballa d'un forma jerarquitzada, per nivells, el nivell zero de la jerarquia són uns rellotges atòmics que estan connectant a uns servidors als quals mantenen sincronitzats. Al mateix temps aquests servidors (nivell 1) mantenen en sincronia uns altres servidors i així successivament.

En el cas de l'arquitectura Skolelinux, el servidor principal es sincronitza amb algun servidor extern, per així mantenir sempre l'hora del sistema actualitzada. A partir d'aquí, qualsevol altre component de l'arquitectura es sincronitza contra el servidor principal, que és suposa que estarà ben configurat.

Algorithm 3 Fitxer de configuració del protocol ntp

```
##########################################
## /etc/ntp.conf
##
## Sample NTP configuration file.
## See package 'xntp-doc' for documentation, Mini-HOWTO and FAQ.
## Copyright (c) 1998 S.u.S.E. GmbH Fuerth, Germany.
##
## Author: Michael Andres, <ma@suse.de>
##
##########################################
[...]
##
## Outside source of synchronized time
##
server ntp # Server IP address/DNS name
##
## Miscellaneous stuff
##
driftfile /var/lib/ntp/drift/ntp.drift # path for drift file
logfile /var/log/ntp # alternate log file
[...]
```

En l'algorisme 3, es pot veure la configuració del fitxer */etc/ntp.conf*, responsable de configurar el protocol NTP dins l'estació de treball. Cal notar que a l'hora de configurar l'adreça del servidor, amb el qual s'ha de sincronitzar l'estació de treball, s'ha utilitzat el nom configurat al DNS en comptes d'utilitzar l'adreça IP directament. L'hora de l'estació de treball es sincronitza amb la del servidor principal a l'arrancar el sistema, en el cas que aquesta estació romangués molt temps encesa, es corre el risc de que el rellotge es dessincronitzi, per tant s'ha afegit el següent codi al crontab per mantenir l'estació en hora.

```
01 * * * * /usr/sbin/ntpdate ntp >/dev/null 2>&1
```

El cron d'un sistema linux és un administrador de processos que s'executa en segon pla, encarregat d'executar tasques a intervals regulars. En aquest cas, executarà la sincronia de l'estació de treball ver el servidor principal cada hora.

4.4.4 Configuració LDAP

El protocol LDAP [lda93] és un protocol a nivell d'aplicació, que funciona sobre el protocol TCP/IP, permetent l'accés a un servei de directori on objectes amb atributs similars estan ordenats i distribuït d'una forma lògica i jeràrquica. És un protocol ideal per buscar informació molt diversa en un entorn de xarxa.

En el cas de l'arquitectura Skolelinux, hi ha un servidor LDAP configurat al servidor principal que conté la informació relativa a usuaris, components hardware de l'arquitectura, directoris, i un llarg etcètera. Cal dir que la gestió del servidor LDAP es duu a terme de forma centralitzada i mitjançant la interfície gràfica de l'aplicació Webmin, la qual cosa simplifica molt la seva gestió. Tot i això, la configuració d'un servidor LDAP és una feina molt complexa que s'escapa de l'abast d'aquest projecte, només comentar que cada entrada del directori, identificada per un identificador únic anomenat DN, consta d'un conjunt d'atributs. En el cas de l'arquitectura Skolelinux, l'identificador és dn: dc=skole,dc=skolelinux,dc=no i els atributs són els noms dels usuaris, PCs, grups d'usuaris,etc.

En el cas de l'estació de treball, durant la instal·lació del sistema operatiu es va crear només un usuari, l'administrador de l'estació, el qual s'autentica a l'estació de forma local mitjançant el fitxer */etc/passwd*. En aquest punt s'ha de donar d'alta un forma alternativa i centralitzada de donar permís als usuaris per accedir al sistema, s'ha de configurar l'accés al LDAP del servidor principal, en la figura 19 es pot veure la interfície gràfica de configuració.

En el cas que la interfície gràfica no oferís la possibilitat de configurar tots els paràmetres, la resta d'opcions avançades es poden trobar el el fitxer

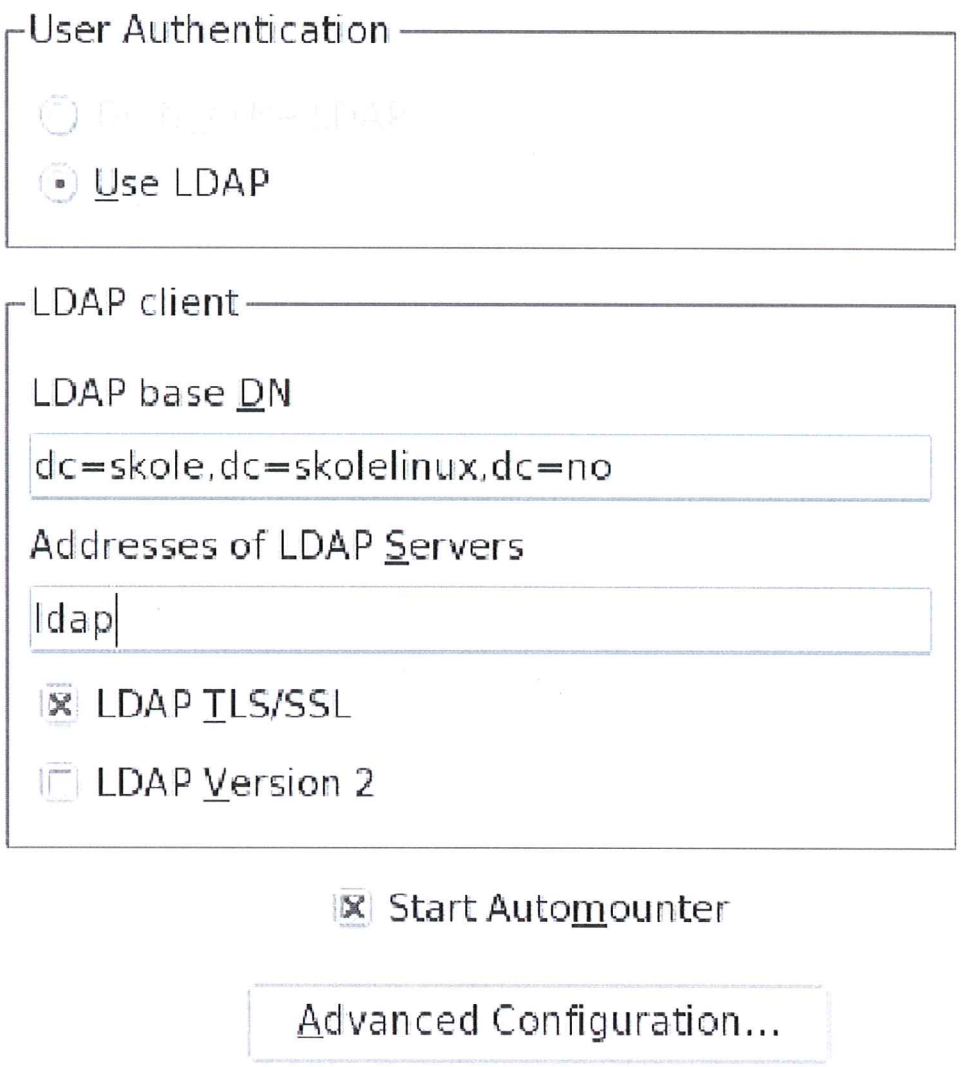

Figure 19: Configuració autenticació remota LDAP

de configuració del sistema. A partir del moment que s'ha acabat de configurar l'accés al servidor LDAP, cap usuari que no estigui donat d'alta al servidor central podrà entrar al sistema, l'única excepció és l'administrador del sistema, l'usuari root, que s'autentica de forma local.

Així doncs per donar d'alta un usuari caldrà accedir a l'eina webmin del servidor central (imatge 20) i procedir a introduir-lo al sistema. Duent a

terme la gestió d'usuaris de l'arquitectura Skolelinux de forma centralitzada guanyem en facilitat de manteniment i en accés lliure al sistema. És a dir, un usuari donat d'alta un sol cop al sistema i amb permisos per accedir-hi, podrà loguejar-se des de qualsevol estació de treball, client lleuger, etc. accedint a tots els serveis. A més a més, els usuaris és poden i de fet es tracten en grups i l'operació de donar o treure permisos d'un grup es propagada directament a tots els usuaris d'aquell grup. Si no existís aquesta gestió centralitzada, la gestió dels usuaris seria molt feixuga, ja que el procés d'introducció d'un usuari s'hauria de repetir per cada component de l'arquitectura.

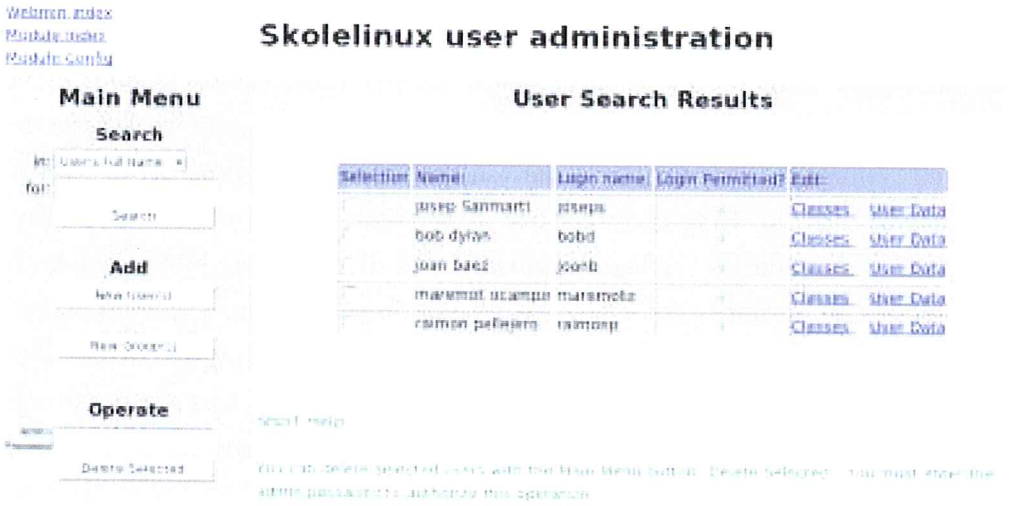

Figure 20: Interfície webmin per donar d'alta un usuari

4.4.5 Configuració d'accés al servidor de fitxers

Dins de l'arquitectura Skolelinux, cada usuari disposa d'un espai físic accessible des de qualsevol terminal que formi part de l'arquitectura, aquest espai a falta d'un nom que l'identifiqui únicament s'ha anomenat servidor de fitxers. En la documentació oficial d'Skolelinux també s'anomena directoris HOME dels usuaris o senzillament $HOME, en aquesta documentació s'utilitzarà qualsevol d'aquestes nomenclatures indistintament. Respecte a l'accés, aclarir que tant si l'usuari es connecta a la xarxa a través d'un terminal amb la configuració de client lleuger com si la connexió es realitzada a

través d'una workstation, l'usuari tindrà accés als mateixos documents. Això es degut a que a cada compte d'usuari se li assigna, en el servidor central, una porció del sistema de fitxers. Aquesta porció, conté la configuració de cada usuari, pàgines web, documents i correu electrònic.

Depenent del tipus de document o del directori on estiguin desats, aquests documents/directoris tindran una sèrie de permisos que els faran accessibles o no pels diferents tipus d'usuaris del sistema. Aquests usuaris del sistema (usuaris de l'arquitectura Skolelinux) es poden dividir en tres grups: El propi usuari, un usuari diferent però que pertany al grup del propi usuari i usuaris que no pertanyen al mateix grup que el usuari en sí.

En l'arquitectura Skolelinux als directoris dels usuaris se'ls hi assigna un nom i un número per identificar-los, on per cada usuari el nom és el mateix i el nombre va augmentant de forma consecutiva. Així es disposa de "home0", "home1", "home2", ... com a identificadors del directori propietat de l'usuari. Hi ha diverses raons per decantar-se per aquest model, entre les quals destaquen les següents: Aquest tipus de directoris juntament amb l'assignació de permisos específics per a cada directori permet que un usuari tingui control total sobre el seu directori però no així sobre els altres. Per altra banda, aquest modelatge juntament amb el fet que tots els directoris dels usuaris es munten en */skole/host/directory/* fa que cada nom sigui únic i irrepetible en tot el sistema.

Per activar el control d'accés a fitxers compartits, cada usuari ha de tindre assignat un grup on no hi hagi cap altre membre. Per fer-ho senzill, el nom d'aquest grup ha d'ésser idèntic al del usuari. Això permet que tot el grup tingui accés a tots els fitxers creats per l'usuari i per tots els membres del grup però com que al grup només hi ha un usuari és aquest l'únic que hi te accés.

El fet d'establir, de bell antuvi, una sèrie de permisos o uns altres al directoris dels usuaris és un fet llargament discutit. Aquesta discusió rau en el fet d'escollir entre assignar permisos de lectura a tothom, podent ésser canviats a posteriori, o negant l'accés a tots els fitxers, fet que implica l'intervenció de l'usuari propietari per a poder canviar els permisos. La filosofia que s'amaga darrere la primera opció és la de compartir el coneixement, més propera als

postulats del software lliure, Open Acces (accés lliure), etc. així com una solució que fa el sistema més transparent. Per altra banda, la segona opció garanteix que no hi haurà accessos no desitjats a informació sensible d'un determinat usuari.

És suggereix que inicialment, el directori d'usuari tingui accés de lectura per a tothom i que sigui el propi usuari qui, dins del directori *home*, crei altres directoris amb permisos o sense per la resta del sistema. Així, pot crear un directori privat (~/priv/) amb permisos únicament per l'usuari (0750) tant de lectura com d'escriptura, i crear un directori públic (~/pub/) amb permisos de lectura per tothom (0775).

En el sistema Skolelinux i, per tant, també en l'estació de treball, els usuaris disposen tant d'un nom d'usuari com d'un grup únics al sistema, per tant la gestió de permisos és força simple. En la taula 3 es poden veure desglossats els diferents permisos tant per un directori públic com per un de privat. La fila corresponent a E_0mostra l'estat inicial dels permisos d'un fitxer corresponent a un usuari del sistema: El propietari del fitxer amb permisos 775 pot realitzar qualsevol operació sobre aquest, en canvi, un altre usuari només te permisos de lectura i execució sobre l'esmentat fitxer. Per altra banda, la fila $E_i$de la mateixa taula mostra quin permisos ha de tindre un fitxer per a que pugui ésser modificat pel seu propietari i, en canvi, no estigui ni visible per la resta d'usuaris del sistema.

Usuari				Grup				Tothom				
R	W	X		R	W	X		R	W	X		
1	1	1	=7	1	1	1	=7	1	0	1	=5	E_0
1	1	1	=7	1	1	1	=7	0	0	0	=0	E_i

Table 3: Permisos de fitxers

Tots i cadascun dels usuaris, a l'hora de donar-los d'alta al sistema, se'ls hi crea automàticament un directori personal anomenar directori HOME amb els permisos descrits anteriorment, com ja s'ha comentat, aquests directoris es guarden en el servidor central. En aquest directori s'hi pot emmagatzemar des de configuracions de programes fins a documents personals, passant per correus o pàgines web. Una de les característiques més importants que han

de complir aquests directoris, és que han d'ésser accessibles des de qualsevulla component de l'arquitectura Skolelinux des d'on un client accedeixi al sistema. És a dir, quan un client accedeix al sistema, automàticament s'ha de muntar el seu directori personal al PC des d'on s'ha connectat, independentment del sistema operatiu i del tipus de dispositiu que sigui.

S'entén per "muntar el directori" el fet de d'accedir al directori $HOME de l'usuari i fer-ne un enllaç a l'estació local, aquest directori està ubicat al servidor central indexat mitjançant el LDAP. En l'algorisme 4 es pot veure l'esquema d'indexació i regles de muntatge emmagatzemades en el LDAP. Aquest sistema de muntatge ha d'ésser totalment transparent a l'usuari i independent del sistema operatiu on s'ha loguejat l'usuari.

Algorithm 4 Indexació dels directoris $HOME en LDAP

```
#ldif automounter information for Skolelinux
#
# Author: Rune Nordb\uffffe Skillingstad <runesk@linpro.no>
# $Id: autofs.ldif 601 2004-06-16 20:45:03Z andreas $
#
# Requires automount.schema
#
# root node for autofs
dn: ou=Automount,dc=skole,dc=skolelinux,dc=no
objectClass: top
objectClass: organizationalUnit
ou: Automount
description: Top node for automount information
# auto.master huh?
dn: ou=auto.master,ou=Automount,dc=skole,dc=skolelinux,dc=no
objectClass: top
objectClass: organizationalUnit
ou: auto.master
```

description: master information for autofs
the /skole mount
dn: cn=/skole,ou=auto.master,ou=Automount,dc=skole,dc=skolelinux,
dc=no
objectClass: top
objectClass: automount
cn: /skole
description: /skole mount point
automountInformation: ldap:ou=skole,ou=Automount, dc=skole,
dc=skolelinux,dc=no
# holder for /skole mount
dn: ou=skole,ou=Automount,dc=skole,dc=skolelinux,dc=no
objectClass: top
objectClass: organizationalUnit
ou: skole
description: holder for /skole mount point
the /skole/tjener submount
dn: cn=tjener,ou=skole,ou=Automount,dc=skole, dc=skolelinux,dc=no
objectClass: top
objectClass: automount
cn: tjener
description: /skole/tjener submount point
automountInformation: -fstype=autofs ldap:ou=tjener,ou=skole,
ou=Automount,dc=skole,dc=skolelinux,dc=no
# holder for /skole/tjener mounts
dn: ou=tjener,ou=skole,ou=Automount,dc=skole,dc=skolelinux,
dc=no
objectClass: top
objectClass: organizationalUnit
ou: tjener
description: holder for /skole/tjener mount point
the /skole/tjener/home0 mount point
dn: cn=home0,ou=tjener,ou=skole,ou=Automount,

dc=skole, dc=skolelinux,dc=no
objectClass: top
objectClass: automount
cn: home0
automountInformation: -rw,rsize=8192,wsize=8192,
intr tjener:/skole/tjener/home0
description: /skole/tjener/home0 mount point

Per tindre accés al servidor de documentació i muntar-lo localment, s'han de configurar diferents serveis en l'estació de treball. Amb l'ajuda de les eines *automount* i *autofs* es configuraran fàcilment els directoris d'usuaris de forma local.

L'eina autofs es l'encarregada de consultar el fitxer */etc/auto.master* (algoritme 5) abans d'analitzar els automounts associats a cada punt de la llista de muntatge. Cada línia del fitxer auto.master és un punt de muntatge i fa referència al fitxer que conté les descripcions del sistema de fitxers que han d'ésser muntats en aquell punt.

Algorithm 5 Fitxer /etc/auto.master

```
# $Id: auto.master,v 1.1 2001/04/17 11:43:02 arvin Exp arvin $
# Sample auto.master file
# Format of this file:
# mountpoint map options
# Also see variable AUTOFS_OPTIONS in /etc/sysconfig/autofs
# For details of the format look at autofs(8).
#/misc /etc/auto.misc
#/misc /etc/auto.misc --timeout=60
#/smb /etc/auto.smb
#/misc /etc/auto.misc
#/net /etc/auto.net
/skole /ldap ou=automount,dc=skole,dc=skolelinux,dc=no
```

Com es pot veure, aquest fitxer configurarà el punt de muntatge /skole. Per a poder accedir als fitxers que hi ha a /skole, l'eina automount haurà de llegir el fitxer /etc/auto.skole (algoritme 6) per trobar les opcions de muntatge i les claus associades al sistema de fitxers. Es pot dir que l'eina

automount treballa des d'un punt inicial de muntatge i amb una llista que descriu les característiques d'aquest punt.

Algorithm 6 Fitxer /etc/auto.skole

```
# $Id: auto.skole,v 1.1 2001/04/17 11:43:02 arvin Exp arvin $
# Sample auto.skole file
# Format of this file:
# mountpoint map options
# Also see variable AUTOFS_OPTIONS in /etc/sysconfig/autofs
# For details of the format look at autofs(8).
skole -fstype=autofs ldap:ou=automount,dc=skole,dc=skolelinux,dc=no
```

Tenint aquests fitxers configurats, tant bon punt un usuari es connecti a l'estació, el sistema verificarà via LDAP la validesa de l'usuari i l'eina automount montarà el directori personal de l'usuari en local. Qualsevol fitxer que crei l'usuari o l'esborri, quedarà creat o esborrat en qualsevol altra sessió que inicii en aquesta estació o en qualsevol altre component de la xarxa. Ja que el sortir del sistema, aquest directori es desmunta quedant llest per a properes sessions.

4.4.6 Servidor d'impressores

L'objectiu d'aquest apartat es arribar a configurar una impressora connectada directament a l'estació de treball i fer-la accessible a tots els components de l'arquitectura Skolelinux. Hi ha molts manuals que expliquen com fer que un ordenador amb GNU/Linux com a sistema operatiu faci de servidor d'impressió per a altres màquines tant amb linux com amb windows. Aquest no serà el cas. Aquí es configurarà el servidor d'impressió amb CUPS[cup99] i per a que sigui utilitzat només per altres màquines que també tinguin instal·lat linux.

Hi ha diverses raons per les quals s'ha optat per configurar el servidor d'impressores així. En primer lloc perquè el 100% dels dispositius que hi ha actualment a l'arquitectura Skolelinux operen amb el sistema operatiu GNU/Linux i per tant, cap dispositiu trauria avantatja del fet que acceptés peticions fetes des d'estacions amb windows. Per altra banda, el poder compartir una impressora amb un client amb windows requereix de la instal·lació

d'un servei extra anomenat Samba[smb92], la qual cosa implica un grau extra de dificultat i un punt que pot provocar errors al sistema. És més la dificultat que portaria la seva configuració que els beneficis que se'n pot treure.

Per altra banda, s'ha de poder compartir una impressora amb un client windows, el fet de negar-ho seria com anar una mica contra la filosofia Skolelinux, on totes les distribucions de sistemes operatius hi tenen cabuda, siguin pertanyents a la branca de programari lliure o no. Tenint en compte aquest fet i sabent que el servidor principal disposa d'un servidor amb samba operatiu, s'aconsella que sigui aquest l'encarregat de compartir impressores per a clients windows. Una altra solució al problema i, de pas reduir la carrega del servidor principal, és la de dedicar una estació de treball a compartir impressores, en tal estació només caldria instal·lar el programari samba i connectar-hi totes les impressores del sistema.

Abans de començar amb la configuració de la impressora, val la pena perdre cinc minuts per saber si la impressora es suportada pel sistema operatiu GNU/Linux. Només cal visitar la web *http://www.linuxfoundation.org/en/OpenPrinting* i buscar la impressora en qüestió.

La configuració de l'estació de treball per a que també actuï com a servidor d'impressió comença per definir al DNS la tupla ≪identificador d'impressió - servidor≫. En aquest cas l'identificador és [ipp], ja que en tot el sistema només hi ha una impressora. Si n'hi hagués més d'una i connectades a diferents dispositius, s'hauria de definir diferents identificadors. Un cop re-activat el DNS, s'ha de començar compartint el servidor d'impressió amb la resta de dispositius de la xarxa. Per tant, en el fitxer de configuració de CUPS (/etc/cups/cupsd.conf) s'afegeixen les següents línies:

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
  Allow From 10.0.2.*
  Allow From 192.168.0.*
</Location>
```

Les quals donen permis per utilitzar la impressora a la pròpia estació de treball, a qualsevol component de la xarxa principal i a qualsevol client lleuger. Per defecte, un cop reiniciat el servei, l'estació de treball publicitarà el servei d'impressió a través del port 631. Qualsevol dispositiu que vulgui imprimir s'haurà de connectar a aquest port mitjançant el seu client d'impressió.

4.4.7 Servidor de copies de seguretat centralitzat

La majoria dels serveis ofertats per el sistema Skolelinux estan centralitzats en el servidor principal, la realització de copies de seguretat no n'és l'excepció. El servei s'executa des de el servidor principal però les copies de seguretat s'emmagatzemen en una estació diferent, es per aquesta raó que es diu que el servei pertany a l'estació de treball. La raó principal per a que les copies de seguretat es guardin en una estació de treball és perquè la majoria de dades sensibles a ésser copiades pertanyen al servidor principal i, en cas que falli aquesta, sempre es tindrà una copia externa d'aquestes configuracions per restaurar l'estació el més ràpidament possible.

El contingut de les copies de seguretat és molt variat i depén en gran mesura de la capacitat d'emmagatzemament del que es disposa. Si la capacitat d'emmagatzemament és molt poca les dades a realitzar copies de seguretat han d'ésser les més sensibles, començant per el contingut dels directoris personals dels usuaris i continuant per les configuracions dels diferents serveis. Si, per contra, la capacitat d'emmagatzemament no és un handicap es poden dur a terme copies de tota la configuració de la xarxa Skolelinux o fins i tot guardar copies de les imatges ISO. Una altre tema que afecta directament a la capacitat d'espai disponible és la definició de períodes de validesa per les copies de seguretat, depenent de l'espai disponible les copies es guardaran un període molt curt, si no hi ha espai, o molt de temps si l'espai en disc no importa.

Per tot això i per molt més, la realització de copies de seguretat no és una opció més, cada cop més esdevé una obligació i grans empreses i destinen molts recursos a la seva realització i manteniment. El projecte Skolelinux no

n'és una excepció i s'ha dedicat un servei específic a tal efecte, en la imatge 21 es pot veure la interfície de l'eina webmin per a configurar el servei de backup. Ara bé, la realització de copies de seguretat sense un estudi previ de quines dades són sensibles i necessiten ésser guardades no serveix de res, s'ha d'haver definit una política de seguretat que tingui en compte tots els factor, des de la quantitat d'espai disponible fins als períodes de manteniment.

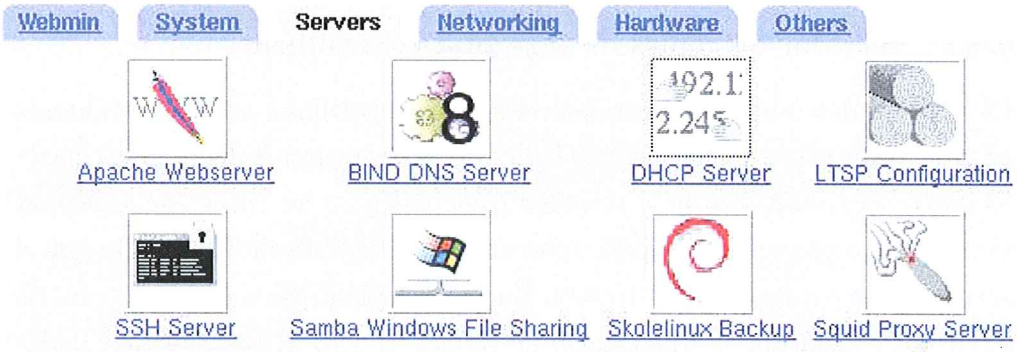

Figure 21: Eina de configuració del servei de backup

Pel que fa a la realització de copies de seguretat en l'estació de treball, cal dir que no hi ha molt espai disponible, és més aviat un recurs escàs i s'ha optat per guardar només les dades més sensibles. Aquestes dades són les que pertanyen als usuaris i estan en els seus directoris personals, per tant es realitzaran copies de tots els directoris $HOME dels usuaris. La principal raó per haver escollit aquesta política de copies és perquè aquestes són les úniques dades de les que no hi ha cap altra copia, les instal·lacions i configuracions es poden tornar a realitzar però la pèrdua de les dades dels usuaris seria, en molts casos, irreparable.

El perìode que s'ha definit per mantenir les copies de seguretat variarà depenent de la quantitat d'usuari i del volum de dades a guardar per cada usuari. Així, si en el sistema hi ha pocs usuaris i la capacitat dels seus directoris es baixa, les copies de seguretat es mantindran durant més temps que si hi ha molts usuaris i amb moltes dades. Segons uns determinats paràmetres s'ha creat un fòrmula que mostra, d'una manera entenedora, la quantitat de dies que es podran guardar les dades en les copies. Així es te que $t = \frac{E_t}{U*v}$ on:

t és el temps en dies per guardar una determinada copia de seguretat fins que una de nova la reemplaci.

$\mathbf{E}_t$ és l'espai total disponible per realitzar copies de seguretat.

U és el nombre d'usuaris del sistema.

v és l'ocupació promig en MBs dels usuaris.

El punt crític és quan $t < 7$ dies, és a dir, el punt que la vida d'un cert document és inferior a 7 dies en les copies de seguretat. És creu que un període de latència inferior a aquest valor no és adequat i, per altra banda, no hi ha cap màxim definit. Actualment s'està parlant molt de preservació de documents al llarg dels anys, això no és més que guardar copies de seguretat i tindre mecanismes per recuperar les dades durant un temps infinit.

Per a configurar l'eina de backup que per defecte hi ha disponible en l'arquitectura Skolelinux, cal configurar en primer lloc aquest servei al DNS, amb l'identificador [backup]. La configuració del mòdul de backup és molt simple, en els següents punts es detallen els paràmetres de la seva configuració:

- Cal definir el moment del dia quan es durant a terme els backups, per defecte hores on la càrrega del sistema és mínima, normalment a la nit.
- S'han de definir els directoris a fer copies de seguretat dels diferents components de l'arquitectura. Tal com s'ha dit, només es duen a terme backups dels directoris dels usuaris, per tant el backup només s'ha d'executar contra el servidor principal.
- Lloc on s'emmagatzemen les copies. S'ha creat un directori especial en l'estació de treball on s'aniran guardant tots els fitxers corresponents a les copies.
- Nombre de dies que s'han de mantenir els backups. Es disposa de: Unes 5Gb d'espai lliure, actualment hi ha molts pocs usuaris (5) i 50 Mb d'ocupació mitja, tot això dona un període màxim de latència de

20.48 dies. Per a que hi hagi una mica de marge de maniobra en cas que el contingut dels directoris augmenti molt i molt ràpidament es defineix un període de 15 dies. S'han de revisar i actualitzar periòdicament totes aquestes dades i modificar els períodes en conseqüència, d'això depén el correcte funcionament del servei de copies de seguretat.

Per a que el mòdul de realització de backups pugui treballar correctament, el servidor central ha de tindre accés, a través del protocol SSH, a tots els altres components de l'arquitectura Skolelinux. Aquest accés ha d'ésser amb permisos d'usuari administrador (root), per així poder realitzar copies de qualsevol directori, sense importar els permisos d'accés.

4.4.8 Configuració SSH

Un dels serveis més útils que s'han configurat en aquesta estació és el ofereix el SSH [ssh95]. Aquest protocol dona la possibilitat d'accedir remotament a l'estació de treball, ja sigui per realitzar tasques de manteniment o per configurar algun servei. Aquestes són les tasques més comuns que es duen a terme amb aquest protocol, encara que també suporta tunneling [2], reenviar ports TCP i connexions X11; també pot transferir fitxers utilitzant els protocols associats SFTP o SCP.

Per defecte aquest protocol escolta les peticions que arriben de connexió pel port 22 però es pot canviar per qualsevol altre. Normalment aquest port es canvia per raons de seguretat, hi ha molts atacs per part de robots al port 22 i el fet de canviar-lo dona un grau extra de seguretat a l'estació. En aquest cas no s'ha modificat, ja que aquesta estació només es pot accedir des de l'interior de la xarxa Skolelinux i no s'esperen gaires atacs des de l'interior de la pròpia xarxa. Per evitar els atacs provinents de l'exterior ja es disposa d'un tallafoc a l'entrada del sistema.

Els usuaris que entren al sistema a través del protocol SSH s'autentiquen de forma local, és a dir, un usuari que vol accedir al sistema cal que estigui donat d'alta com a usuari local de l'estació de treball, en el fitxer */etc/passwd*.

[2] El terme anglès "tunneling protocol" s'utilitza per descriure el procés on un protocol de xarxa es encapsulat en un protocol diferent per a ésser transmés.

No obstant, mitjançant el fitxer */etc/ssh/sshd_config* es pot configurar que els usuaris s'autentiquin via LDAP, com qualsevol altre usuari del sistema. No s'ha cregut necessari realitzar l'autenticació dels usuaris via LDAP, ja que aquest protocol te poca utilitat per usuaris que no siguin administradors i seria un problema més que una avantatja.

4.4.9 Configuració CDs/DVDs

Degut a que els components de l'arquitectura Skolelinux configurats com a estacions de treball són més modern que la resta, solen tindre més dispositius externs, ja siguin lectors de disquets o d'unitats òptiques com ara CDs o DVDs. Avui en dia, qualsevol dispositiu disposa d'aquests tipus de perifèrics, no obstant a continuació es descriuran els passos a seguir per configurar un dispositiu òptic i compartir-lo amb la resta de PCs que formen l'arquitectura Skolelinux.

El primer pas a realitzar és muntar el dispositiu òptic per a que funcioni el local, només en l'estació de treball. Es busca el dispositiu (/dev/hdc), es dona permisos per a que pugui ésser muntat per un usuari no administrador i es munta el tipus de sistema de fitxers, en aquest cas udf per a DVDs i iso9660 per a CDs.

```
mount -t udf,iso9660 -o user /dev/hdc /export/cdrom/
```

Un cop el dispositiu òptic funciona correctament, cal afegir al fitxer */etc/exports* la ruta del directori que es compartirà amb la resta de la xarxa, en aquest cas /export/cdrom. Un cop definit s'executa la següent comanda amb els següents resultats.

```
exportfs
/export/cdrom <world>
```

En aquest punt, el dispositiu òptic funciona correctament, s'ha definit el directri d'exportació i ara només cal arrancar el servei NFS[nft84] per a que es facin efectius aquests paràmetres d'exportació.

```
/etc/init.d/nfsd restart
* Stopping NFS mountd [ OK ]
* Stopping NFS daemon [ OK ]
* Stopping NFS services [ OK ]
* Starting NFS services [ OK ]
* Starting NFS daemon [ OK ]
* Starting NFS mountd [ OK ]
```

Ara només cal publicitar el port que oferirà el servei NFS en l'estació, això es duu a terme mitjançant el servei portmap. Primer però cal definir qui ha de tindre accés als recursos publicitats mitjançant el fitxer /etc/hosts.allow. En principi qualsevol dispositiu de l'arquitectura hauria de poder accedir al recurs publicitat, per tant s'ha d'afegir:

```
portmap:10.0.2.0/255.255.255.0
portmap:192.168.0.0/255.255.255.0
```

Que són les adreces IP dels dispositius de la xarxa principal i dels clients lleugers i, per finalitzar, es guarda el fitxer i es reinicia el servei portmap.

```
/etc/init.d/portmap restart
* Stopping portmap daemon... [ OK ]
* Starting portmap daemon... [ OK ]
```

Qualsevol dispositiu extern que desitgi accedir al servei d'accés a dispositius òptics, només cal que munti en local els directoris publicitats. La comanda per visualitzar quins directoris són accessibles és showmount -e <wkssuse.intern | IPw>, on wkssuse és l'identificador de l'estació de treball definit al DNS. Així en local, cal crear un directori (/mnt/dispoptic) per a tindre el contingut del dispositiu òptic i executar:

```
mount -t nfs wkssuse:/export/cdrom /mnt/dispoptic
```

Si es desitja que cada cop que es reinicii un PC, el dispositiu òptic estigui accessible en l'estació local, cal afegir l'anterior comanda al fitxer */etc/fstab* quedant:

```
wkssuse:/export/cdrom /mnt/dispoptic nfs user,exec,dev,nosuid,rw,noauto
0 0
```

4.4.10 Configuració de diferents servidors

Tenint en compte que aquesta estació s'ha de comportar com un component més de l'arquitectura, és necessari l'accés a diferents serveis extern, ofertats pel servidor principal. Aquests serveis són tant variats com:

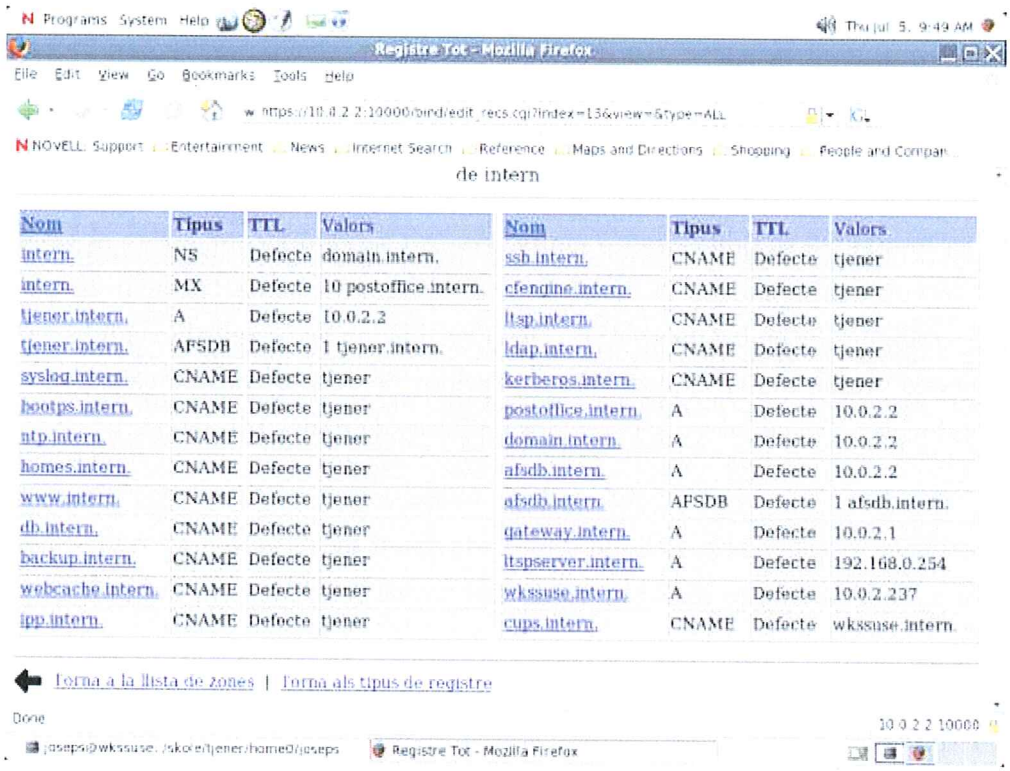

Figure 22: Llistat de serveis configurats al DNS

- Servidor de correu: Per defecte es configura el Limacute, servidor de correu de molt fàcil configuració i utilització. En la seva configuració cal afegir el nom que se li assigna per defecte ([postoffice]) al servidor de DNS i ja passa a ésser accessible des de qualsevol component de l'arquitectura.

- Servidor de pàgines web: Probablement el servidor de contingut web