

Capítol 3

El Servei SAMBA
Configuració del servei
Escenaris de xarxa: un cas real

3.1 El Servei SAMBA

Des de la pàgina WEB de SAMBA [1] es defineix el servei com : “Una suite de programes (dos servidors *smbd* i *nmbd*, i una sèrie d'aplicacions) que permet compartir fitxers i impressores cap a clients que suportin els protocols SMB/CIFS (Server Message Block, Common Internet File System)”. Això vol dir que SAMBA permet la transferència de fitxers i informació entre sistemes UNIX/Linux i els que estan basats en Windows i que donen suport als protocols SMB/CIFS.

En realitat, SAMBA, amb la seva versió 3.0 estable ja publicada, permet algunes coses més. De fet, el principal avantatge que presenta la suite SAMBA és el fet de ser pràcticament equivalent a qualsevol servidor SMB/CIFS (Windows NT o 2000, Servidor Netware, servidor NFS UNIX, ...) però amb la particularitat de ser Software Lliure i gratuït: és a dir que no hi ha cost afegit per llicències d'ús ni a servidors ni a clients, i que qualsevol persona pot accedir al codi font, disposar-lo i modificar-lo en compliment de la llicència GNU. Però no cal ser tant optimistes. Siguem realistes i mirem què i què no permet fer SAMBA en substitució d'altres sistemes de pagament (com ara els sistemes de Microsoft); observem la taula següent:

Utilitat	Ho pot fer?
Servidor de Fitxers	Sí
Servidor d'impressores	Sí
Servidor DFS de Microsoft	Sí
PDC	Sí
BDC	No
Controlador de Domini Active Directory	No
Autenticació Windows 95/98/Me	Sí
Autenticació Windows NT/2000/XP	Sí
Local master browser	Sí
Local backup browser	Sí
Master Broser de Domini	Sí
Servidor WINS Primari	Sí
Servidor WINS Secundari	No
Atenticació UNIX/Linux	Sí
Integració LDAP	Sí

Així, podem afirmar que SAMBA és un bon substitut per un servidor de domini que no utilitzi la tecnologia Active Directory per les raons següents:

1. És gratuït com a servidor a diferència de les llicències de xarxa que imposa Microsoft en els seus productes similars.
2. Treballa sota l'entorn del sistema operatiu UNIX/Linux, amb el que es fa hereu de la seva estabilitat i millora en funcionament enfront d'altres sistemes.
3. Té una bona resposta en xarxes heterogènies on es barregen diferents SO clients.

Referent a les seves prestacions com a client: es pot integrar en qualsevol esquema de xarxa per validar els usuaris, treballant d'igual a igual amb la resta de clients de la xarxa, i permetent d'aquesta manera que es comparteixin recursos locals com ara fitxers i impressores. En els esquemes de xarxa Linux, SAMBA està prenent una nova orientació: la validació d'usuaris. El fet d'utilitzar bases de dades comunes d'usuaris i grups, entre diferents sistemes operatius, permet als administradors de xarxa simplificar el manteniment i optimitzar la gestió dels permisos augmentant la seguretat. Avui en dia, SAMBA permet la utilització de la seva base de dades d'usuaris per la validació de sistemes UNIX/Linux i Windows. En el mateix sentit, a la darrera versió de SAMBA s'ha optat per la integració amb LDAP [2] (Lightweight Directory Access Protocol) per la gestió i manteniment dels usuaris, grups i els seus permisos.

Tot el que aquí explicaré sobre SAMBA es pot trobar a la documentació oficial del projecte i a diversos llibres que versen sobre el tema [3]. No entraré a fer una descripció detallada de tot el que és SAMBA. En canvi, el que farem, seguint la filosofia de la distribució, és treballar sobre exemples concrets per veure quina és la utilitat que en podem treure en l'empresa: com implementar el servei i les eines que tenim per fer l'administració de la xarxa més simple.

3.2 Usuaris, grups i permisos: escenaris de xarxa interna

Imaginem una empresa d'una mida mitjana, dedicada a la creació de documentació i activitats multimèdia, amb uns 15 llocs de treball basats en sistemes heterogenis: Microsoft Windows NT/2000/XP, UNIX, Linux, MacOS. Això no és casual, resulta que diferents departaments de l'empresa necessiten utilitzar aquests sistemes degut als recursos i programes que utilitzen en la seva feina diària:

- La comptabilitat es gestiona en un sistema UNIX utilitzant una aplicació escrita en COBOL i que està en funcionament des de fa molts anys. Els usuaris es connecten al sistema per mig de terminals de text.
- Utilitzen els ordinadors Apple per l'edició i maquetació de documentació i propaganda de l'empresa.
- Els clients Windows s'utilitzen per finalitats ofimàtiques i per la connexió a certes pàgines que únicament funcionen correctament amb aquest sistema.
- Els clients Linux s'utilitzen com a “camp de proves” per la publicació en local de les activitats Web i multimèdia que s'han desenvolupat i, alguns, com a eines de programació i explotació de bases de dades (PHP+MYSQL, Perl, Python, C).

Actualment es disposa d'un servidor de fitxers i impressores basat en un Windows 2000 Server amb un número de llicències de xarxa que ja estan complertes amb els clients Windows que s'utilitzen actualment i que es validen al servidor. Els problemes als que s'enfronta l'administrador són:

1. Ha de disposar de diverses bases de dades d'usuaris i grups duplicades segons el sistema operatiu usat i vol que això s'acabi, ja que els usuaris han de canviar sovint de màquina per realitzar tasques diverses. També vol definir una política de permisos globals i compartir certes zones del servidor perquè “tots” els usuaris hi puguin accedir per mig de la xarxa interna. Vol optimitzar l'ús de les impressores. L'administrador voldria utilitzar un esquema el més semblant a la xarxa controlada per el servidor 2000 però que englobes a totes les màquines.
2. Ha de decidir si amplia el número de llicències de xarxa del servidor Windows 2000 ja que s'enfronta amb una ampliació dels llocs de treball en un futur proper.
3. Voldria, per finalitzar, una gestió el més personalitzada possible dels usuaris amb perfils mòbils, carpeta dedicada al servidor i altres coses com ara connexions a unitats de xarxa personalitzades.

Mirem que ens pot aportar o costar migrar el Servidor Windows 2000 a un servidor Linux amb SAMBA (i altres serveis) integrat:

1. El cost de maquinari és nul ja que partim del principi de que un Servidor 2000 de Microsoft necessita el doble de recursos que un servidor Linux [4].
2. No cal fer cap despesa addicional en programari ni en llicències ja que GNU/Linux i SAMBA són lliures i gratuïts.
3. SAMBA ens permet una gestió centralitzada dels usuaris de la xarxa en el servidor Linux amb una única base de dades que serà utilitzada per tots els clients SMB/CIFS, inclosos el sistema UNIX i MacOS.

4. SAMBA ens permet la utilització de perfils mòbils (de Microsoft) per als usuaris, i l'assignació directa de la zona d'usuari Linux com a recurs de xarxa personalitzat per cada usuari (això bé configurat així per defecte des de la versió 2.0 de SAMBA).
5. Podem utilitzar una política de seguretat (amb el que respecta als recursos compartits del servidor) basada en dos esquemes: segons els permisos UNIX/Linux (l'estàndard en versions anteriors a la 3.0 i que es manté actualment) i utilitzant permisos particulars de la suite SAMBA. L'esquema basat amb els usuaris i grups de UNIX/Linux és evidentment més segur i fiable que el que s'utilitza en sistemes basats en windows.
6. SAMBA ens permet definir fitxers d'execució per lots personalitzats per usuari, grup i en general per tots els usuaris de la xarxa, amb el que la flexibilitat en el que es refereix a la personalització de l'entorn està assegurada.

Com es pot extreure, la migració des del programari propietari a GNU/Linux aporta un ventall d'avantatges molt interessant per resoldre les necessitats del cas anterior. Resulta més econòmic i presenta funcionalitats que la solució amb altres sistemes no tenen. S'intueixen algunes utilitats potencials, que si bé en primera instància no són necessàries, podrien donar servei a l'empresa en el futur i, el més important, sense cost afegit. En referència als costos d'implantació de la solució ja s'ha vist que no hi ha despeses en maquinari ni en llicències; en canvi, la despesa més important serà en capital humà “expert” per dur a terme la migració i en formació del personal responsable de l'àrea d'informàtica. Seguidament exposaré un cas “real” d'implantació de servidor Linux en un entorn de xarxa complex com és un centre d'educació secundària.

3.3 SAMBA PDC en una xarxa mixta Windows/Linux

Ens enfrontem amb un cas concret que correspon a la xarxa d'un centre d'educació d'una mida mitjana-gran i amb unes necessitats molt ben marcades:

1. Uns 1200 usuaris (1000 alumnes, uns 200 professors equip directiu i PAS inclosos). Validació centralitzada dels usuaris als servidors.
2. Separació físicament els servidors dedicats a alumnes, professorat i gestió del centre. La política de seguretat ens indica que la jerarquia de permisos va de més a menys, des dels usuaris de l'equip directiu, seguit dels professors i finalment els alumnes. És a dir, que una vegada un component de l'equip directiu es valida en el servidor de gestió pot accedir als servidors de professorat i alumnat sense problemes. Un professor que es valida en el servidor de professorat pot accedir al servidor de l'alumnat però no al servidor de gestió. Finalment, un alumne es pot validar en el servidor de la intranet de l'alumnat però no pot accedir a la xarxa de professorat ni de gestió.
3. Existència de grups d'usuaris amb jerarquies molt marcades (política de permisos: alumnes, professors, departaments, equip directiu, administradors de xarxa). Recursos compartits amb permisos determinats per l'usuari i el grup, on les polítiques de creació de fitxers i directoris assegurin la seva continuïtat. Dins d'un servidor hi ha recursos compartits que són accessibles (lectura o lectura/escriptura) a uns usuaris i a altres no, segons la política de seguretat que marquem. Els nous directoris i fitxers hauran de conservar aquests permisos.
4. Necessitat d'utilitzar perfils mòbils per als usuaris a les aules d'informàtica i la resta de dependències. Els usuaris tenen un gran mobilitat en el que respecta a la seva estació de treball, no sol ser fixa, per tant, la seva informació personal haurà d'estar disponible estiguin a l'estació de treball que estiguin.
5. Gestió i control “senzilla”, per part de l'administrador de la xarxa, de tots els processos oberts en un instant determinat.

6. Les màquines client presenten sistemes operatius basats en Windows (2000/XP) i algunes aules de cicles formatius tenen sistemes Linux amb arrancada dual. Cal donar suport al mateix temps a tots els tipus de clients Windows o Linux.

Abans de continuar endavant és necessari comentar que la solució complerta a tot el que es demana en la llista anterior no passa únicament per la utilització de SAMBA. Hi ha una bona part, la que correspon a la seguretat entre xarxes, que està controlada per tallafocs amb regles IPTABLES. Aquí utilitzarem per fer això les eines que ens ofereix SAMBA, que són: la validació d'usuaris i l'emissió dels paquets per part del servidor a un tram de xarxa particular. Els servidors que utilitzarem per dur a terme aquesta configuració cal que tinguin aquestes característiques:

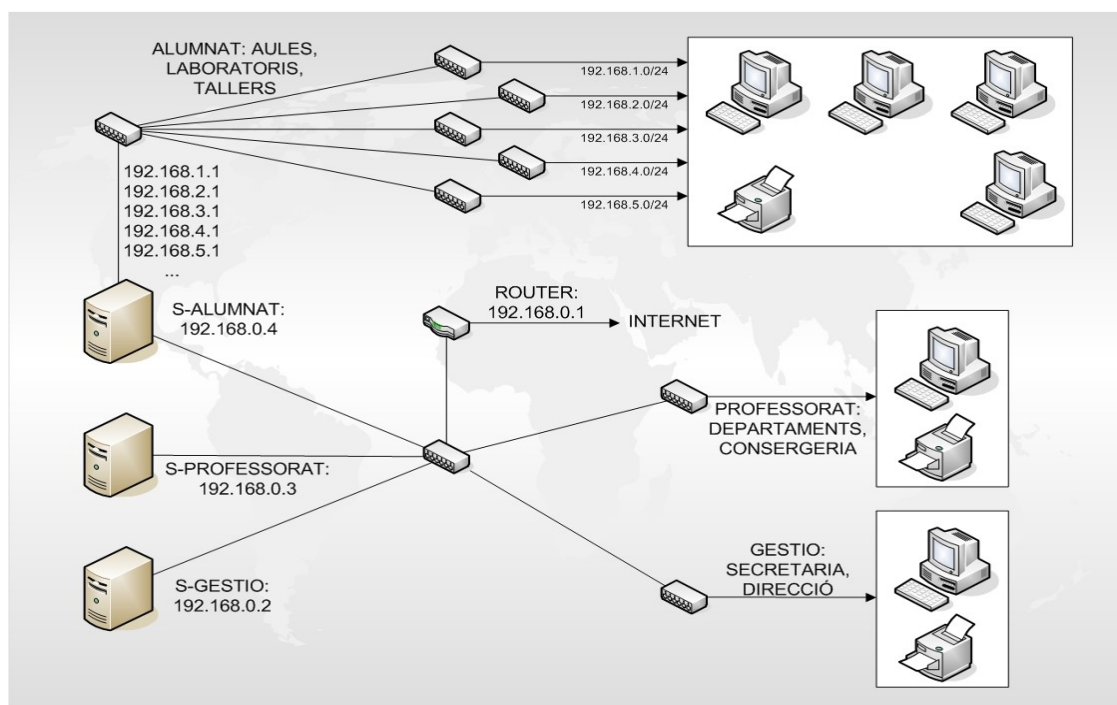
1. Un servidor de bones proporcions per al PDC que controlarà tots els usuaris del centre: dues targetes de xarxa i una zona de disc respectable. Un exemple concret (que actualment està en funcionament a l'IES SEP de l'Ebre de Tortosa) podria ser:

- ✓ Placa: Intel dual per a processadors XEON amb SATA i amb capacitat per 8 GB de RAM. Assegurem l'escalabilitat (ampliació del servidor)
- ✓ Processador: 1 XEON a 3.0 Ghz
- ✓ Memòria RAM: 1 GB DDR ECC
- ✓ Discos: 2 Discos SATA 200 GB + 1 Disc PATA 200 GB

2. Els servidors de gestió i professorat que no cal que siguin tan escalables. Per l'exemple concret de l'IES SEP de l'Ebre són:

- ✓ Placa: MSI monoprocessador per PIV (o AMD) amb SATA i amb capacitat per 4 GB de RAM.
- ✓ Processador: 1 Pentium IV a 2.8 Ghz
- ✓ Memòria RAM: 1 GB DDR ECC
- ✓ Discos: 2 Discos SATA 200 GB + 1 Disc PATA 200 GB

Les IPs de les targetes de xarxa estan configurades tal com s'observa en la següent figura:

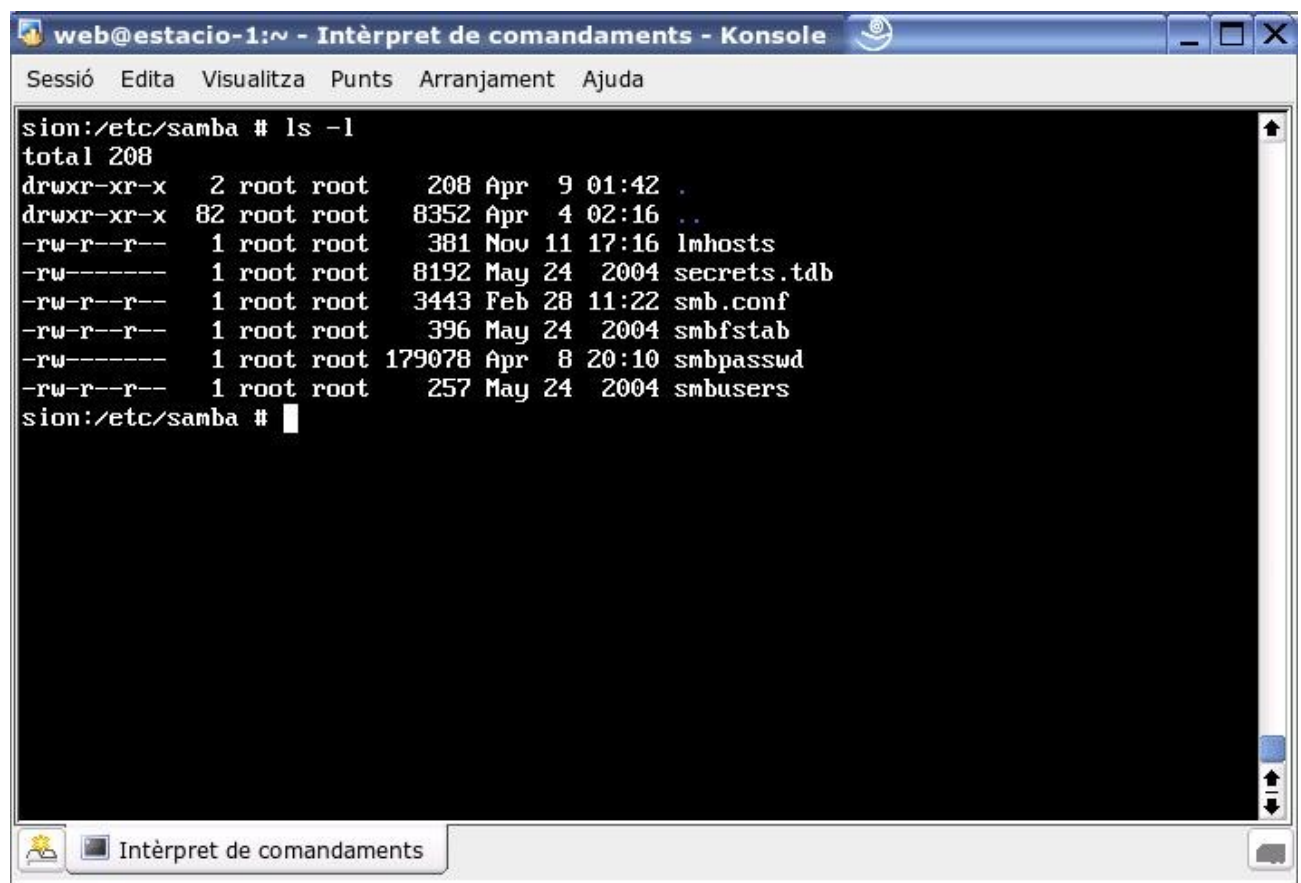


Tots tres servidors comparteixen connexió a un mateix concentrador on trobem la connexió a l'encaminador i a la resta d'aparells de connexió que corresponen a dependències del professorat (departaments, consergeria) i de gestió (secretaria, direcció). La segona targeta de xarxa del servidor principal (alumnat) connecta a un altre concentrador, independent del primer, on es fan arribar les connexions de les dependències corresponents a l'alumnat (aules, laboratoris, tallers). La targeta de xarxa secundària del servidor principal té IPs múltiples, una per cada part diferenciada de l'edifici (diferents nivells). D'aquesta manera ens assegurem un rang prou ampli per cobrir totes les necessitats d'ampliació futures i introduïm una pauta d'organització.

Com es pot observar a l'esquema anterior, les comunicacions de totes les màquines connectades des del servidor principal cap a les dependències de l'alumnat hauran de passar pel servidor "obligatòriament". Això ens permetrà filtrar, controlar el tràfic de xarxa, l'accés cap al router i a la resta de la xarxa interna del centre. Amb les eines adequades podrem tenir un control important del tràfic, com ja veurem als capítols 6 i 7 amb el servidor SQUID i el tallafocs de Linux IPTABLES.

3.3.1 Configuració de SAMBA

Els fitxers de configuració de SAMBA es solen trobar en la majoria de distribucions sota el directori */etc/samba*. A continuació observem un llistat dels fitxers sota aquest directori per la versió 3.0 de SAMBA:



```

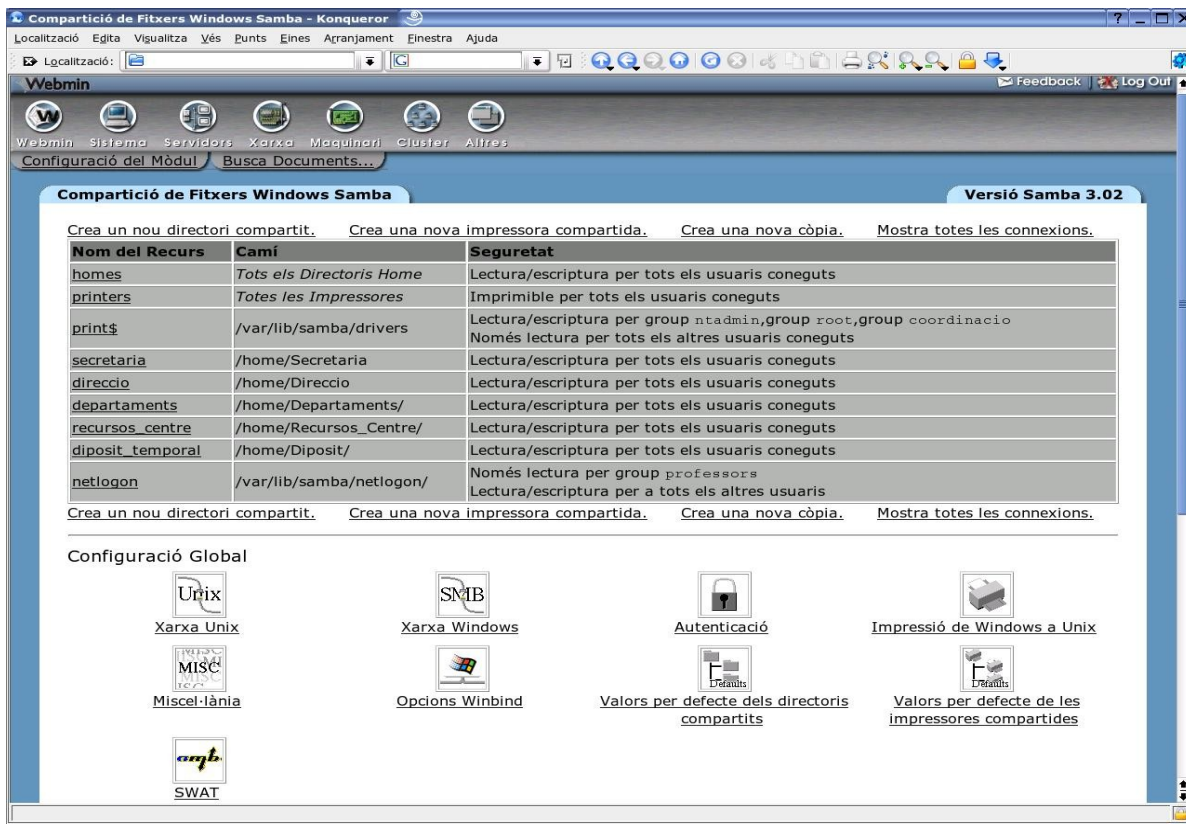
web@estacio-1:~ - Intèrpret de comandaments - Konsole
Sessió  Edita  Visualitza  Punts  Arranjament  Ajuda

sion:/etc/samba # ls -l
total 208
drwxr-xr-x  2 root root   208 Apr  9 01:42 .
drwxr-xr-x 82 root root 8352 Apr  4 02:16 ..
-rw-r--r--  1 root root   381 Nov 11 17:16 lmhosts
-rw-----  1 root root 8192 May 24 2004 secrets.tdb
-rw-r--r--  1 root root 3443 Feb 28 11:22 smb.conf
-rw-r--r--  1 root root   396 May 24 2004 smbfstab
-rw-----  1 root root 179078 Apr  8 20:10 smbpasswd
-rw-r--r--  1 root root   257 May 24 2004 smbusers
sion:/etc/samba #

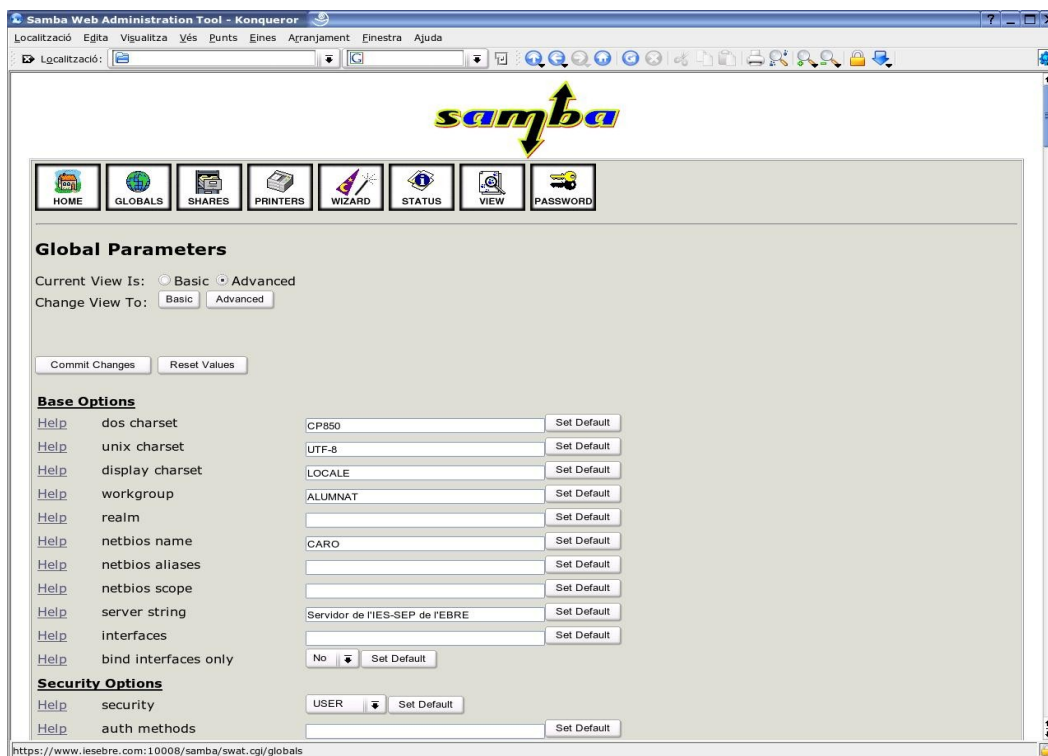
```

El fitxer *smb.conf* conté els paràmetres de configuració del servei SAMBA, mentre que el fitxer *smbpasswd* conté els usuaris de samba generats en el nostre sistema (normalment amb la comanda *smbpasswd*). El fitxer *lmhosts* és l'equivalent a *hosts* per al servidor WINS i que també trobem sovint en els sistemes basats en Windows. *smbusers* ens permet crear una llista d'equivalències entre usuaris windows-linux de la nostra xarxa, de manera que no hi ha una necessitat "real" que els usuaris Linux i Windows coincideixin. De fet aquest fitxer s'usa molt sovint per fer migracions d'entorns Windows existents cap a entorns Linux amb SAMBA.

Podem configurar SAMBA editant el fitxer de configuració (en mode text o des de les finestres amb un editor de text com ara *kate* que no introdueix caràcters addicionals). També podem configurar SAMBA utilitzant WEBMIN i més concretament l'eina de configuració específica via web de SAMBA: *swat*. Cal anar a *Servidors -> Compartició de Fitxers Windows SAMBA -> Swat*:



Una vegada connectats a l'aplicació SWAT anem a l'apartat Globals i escollim l'opció de visualització avançada per veure i canviar la configuració del servidor SAMBA.



També podem configurar SAMBA al Linux SuSE des de YAST: *Servicios de Red -> Cliente o Servidor SAMBA*. Ens permet fer el mateix tipus de manipulacions que amb el servei SWAT.

Mirem el fitxer de configuració del servidor principal de la xarxa que estem configurant. Si mirem el contingut del fitxer de configuració de SAMBA, *smb.conf*, el primer que ens crida l'atenció és que està dividit en seccions encapçalades per una paraula clau: [globals], [homes], [printers] ... en general [nom_del_rekurs_compartit], seguida d'una sèrie de paràmetres relacionats. A la secció [globals] és on es defineixen les principals característiques de funcionament del servei. Al manual de SAMBA hi ha una explicació “detallada” de cada paràmetre i les seves possibilitats. Exposaré únicament els paràmetres que més ens aclariran el funcionament dels nostres servidors. SAMBA, en ell mateix, és un servei susceptible de fer un curs monogràfic (i aquest no és el cas). Mirem en detall la secció [globals] del servidor principal:

```
# Samba config file created using SWAT
# from 0.0.0.0 (0.0.0.0)
# Date: 2004/04/29 20:57:01

# Global parameters
[global]
    netbios name = caro
    server string = Servidor de l'IES-SEP de l'EBRE
    local master = yes
    domain master = yes
    workgroup = alumnat
    os level = 99
    security = user
    encrypt passwords = yes
    passwd backend = smbpasswd
    unix password sync = Yes
    update encrypted = Yes
    wins support = true
    admin users = @coordinacio
    write list = @coordinacio
    read list = @coordinacio
    printer admin = @coordinacio
    add machine script=/usr/sbin/useradd -c Machine -d /var/lib/nobody -s /bin/false %m$
    domain logons = yes
    logon drive = z:
    time server = Yes
    logon script = XARXA.BAT
    veto files = /*.eml/*.*.nws/riched20.dll/*.*}/*.*}
    ldap admin dn = alumnat
    ldap suffix = dc=example,dc=com
    socket options = SO_KEEPAIVE IPTOS_LOWDELAY TCP_NODELAY
    deadtime = 2
    map to guest = Bad User
```

Segons aquests paràmetres, el nostre servidor actuarà com un Controlador Principal de Domini (PDC) del domini **alumnat** i de nom NetBios **caro**. Serà necessària l'autenticació dels usuaris de la xarxa perquè aquests es puguin connectar als recursos compartits, o dit d'una altra manera, el servidor pot actuar com agent d'autenticació dels usuaris de la xarxa. Això vol dir que els clients correctament configurats podran validar usuaris que no estiguin donats d'alta en la seva base de dades d'usuaris local. Una vegada autenticat l'usuari, s'aplicaran les polítiques de seguretat corresponents a cada recurs compartit com veurem més tard. Segons aquesta configuració, els

usuaris que es donin d'alta en el sistema Linux automàticament seran usuaris del servei SAMBA i utilitzaran paraules clau amb xifrat. El nostre servidor serà un servidor WINS primari i el grup d'usuaris pertanyents a "coordinacio" seran administradors de xarxa en el que refereix als recursos compartits (impressores i documents) amb permisos globals per llegir i escriure en qualsevol recurs, independentment dels permisos particulars del mateix. Les màquines que es vulguin unir al domini ho faran de manera automàtica sense intervenció de l'administrador, cosa que és útil si hi ha gran quantitat de clients, però redueix la seguretat de l'entorn. El servidor comparteix la carpeta personal de l'usuari identificat, a la que assigna la unitat local Z:. El nostre servidor és un servidor de temps per els clients Windows i s'executa un fitxer BAT en l'engegada de cada sessió anomenat: XARXA.BAT.

Mirem ara els recursos compartits:

```
[homes]
  browseable = no
  writable = yes
  write list = @coordinacio
  guest ok = no
  comment = Directori d'Usuari
  create mode = 0755
  directory mode = 0755
[recursos_centre]
  comment = Recursos per al professorat
  path = /home/Recursos_Centre/
  write list = @coordinacio
  read only = No
  browseable = yes
[diposit_temporal]
  comment = Zona d'Scratch
  path = /home/Diposit/
  write list = @professors, @coordinacio, @alumnes, @direccio, @administracio
  force user = nobody
  force group = nogroup
  read only = No
  create mask = 0777
  directory mask = 0777
  delete readonly = Yes
  browseable = yes
[netlogon]
  comment = Netlogon NT
  path = /var/lib/samba/netlogon/
  read list = @professors, @alumnes
  write list = @coordinacio
  force user = root
  force group = coordinacio
  read only = No
  browseable = no
```

El recurs [homes] fa referència a la zona d'usuari. És la zona del disc (normalment sota */home*) que el sistema crea per cada usuari en un sistema UNIX/Linux. Normalment, segons la configuració de seguretat del servidor, els permisos per defecte d'aquestes zones d'usuari impliquen que les carpetes i documents es poden visualitzar per part de qualsevol usuari de la xarxa. Encara que aquest fet és interessant si volem poder fullejar el contingut de les carpetes dels nostres usuaris (alumnes) pot ser un inconvenient si no volem que els usuaris puguin fer el mateix entre ells (professors).

Possiblement, la política de seguretat ha d'arribar a un compromís entre uns permisos i els altres. Mirem a la següent imatge quina seria una bona política de permisos per les zones d'usuari del professorat:

```

web@estacio-1:~ - Intèrpret de comandaments - Konsole
Sessió Edita Visualitza Punts Arranjament Ajuda

sion:/home/professors # ls -l /more
total 100
drwxr-xr-x 174 root      root      4488 Apr  8 03:28 .
drwxr-xr-x  15 root      root      1312 Apr  8 03:34 ..
drwx-----x 14 aanguera professors 864 Feb 11 19:10 aanguera
drwx-----x 14 aaragones professors 776 Mar 31 10:43 aaragones
drwx-----x 12 aarasa   professors 688 May  1 2004 aarasa
drwx-----x 14 aaznar   professors 776 Sep 22 2004 aaznar
drwx-----x 22 abonet   professors 1224 Oct 14 11:14 abonet
drwx-----x 12 acastella professors 688 May  1 2004 acastella
drwx-----x 14 acreix   professors 776 Sep  3 2004 acreix
drwx-----x 16 aesteller professors 856 Feb 10 08:54 aesteller
drwx-----x 14 agamundi professors 776 Nov 24 19:32 agamundi
drwx-----x 14 agarcia   professors 776 Oct 13 12:04 agarcia
drwx-----x 12 aguzman   professors 688 May  1 2004 aguzman
drwx-----x 14 aizaguirre professors 776 Sep  3 2004 aizaguirre
drwx-----x 17 alopez    professors 936 Mar  8 20:23 alopez
--More--

```

A la part dreta observem els directoris dels usuaris, amb el mateix nom que s'ha assignat a cada usuari. A la part esquerra podem veure la política de permisos: lectura-escriptura-execució per al propietari i únicament execució per la resta del món. Això evita que qualsevol usuari pugui veure el contingut de les carpetes personals d'un altre usuari professor, a no ser que conegui el nom de la carpeta o document i aquesta tingui permís de lectura de manera explícita (per exemple *public_html*). El que un usuari veurà en l'interior de la seva carpeta personal en l'entorn Linux seria el següent:

```

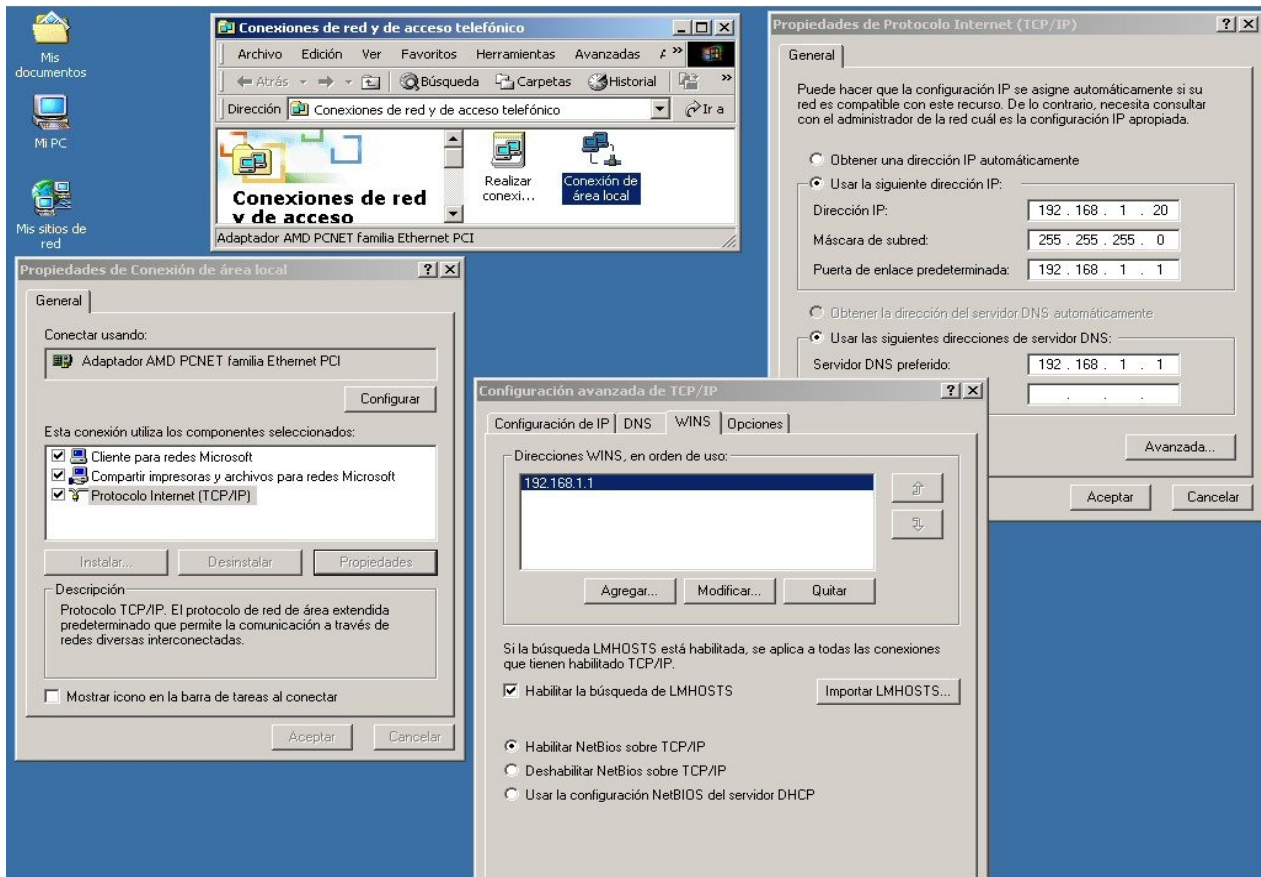
web@estacio-1:~ - Intèrpret de comandaments - Konsole
Sessió Edita Visualitza Punts Arranjament Ajuda

usuari@sion:~> ls -l
total 1
drwx----- 3 usuari users 344 Apr  4 01:12 Desktop
drwxr-xr-x  2 usuari users  80 Apr  4 01:12 Documents
drwxr-xr-x  2 usuari users 600 Apr  4 01:12 bin
drwx----- 2 usuari users 112 Apr  4 01:12 mail
drwxr-xr-x  3 usuari users  88 Apr  4 01:12 profile
drwxr-xr-x  2 usuari users 144 Apr  4 01:12 public_html
usuari@sion:~>

```

La carpeta *Desktop* correspon a l'escriptori de Linux i la carpeta *Documents* la crea el sistema per defecte a l'igual que *bin*, *mail* i *public_html*. Normalment, la carpeta *profile* es crea la primera vegada que un usuari es valida des d'un client contra el servidor i en ella es guarda el perfil mòbil Windows de l'usuari, que després el seguirà allí on vagi dins la xarxa interna si es torna a validar. Mirem ara que cal fer per configurar les màquines que actuaran com a clients. Comencem amb els clients Windows (2000/XP).

La configuració de xarxa d'aquestes màquines haurà de ser adient a la configuració del servidor. El tram d'IP s'haurà d'ajustar a un dels que ofereix el servidor i la porta d'enllaç, el DNS i el servidor WINS únicament podran ser el nostre servidor. Considerem un client del tram IP 192.168.1.0/24, una configuració correcta per aquest tram seria:

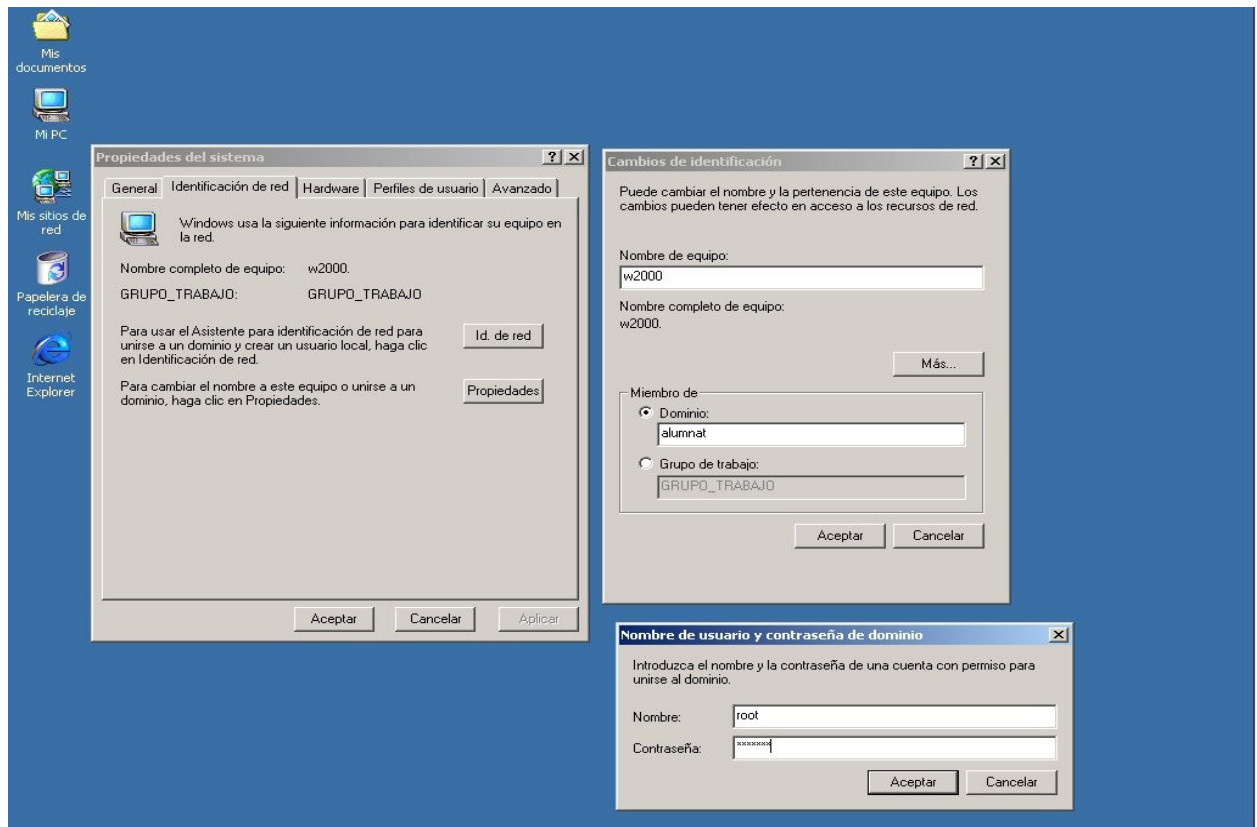


Com es pot veure a la figura, tan la porta d'enllaç com els servidors DNS i WINS corresponen a la IP del servidor principal (192.168.1.1). Ja sabem que el servidor s'ha configurat per ser un servidor WINS primari. Al capítol següent veurem la configuració del servidor DNS i als capítols 6 i 7 veurem com configurem el servidor per actuar d'enrutador. Amb aquesta configuració, el client ja pot comunicar amb el servidor SAMBA i pot veure a l'entorn de la xarxa els recursos compartits. Ens falta, però, validar els usuaris de xarxa al client. Per fer-ho cal que introduïm el client Windows al domini. Si fem un clic amb el botó de la dreta sobre Mi PC i escollim les propietats accedirem a la configuració d'identificació de xarxa del sistema Windows, que és el lloc on configurem si pertany a un grup de treball o en aquest cas a un domini.

Abans, però, ens caldrà donar d'alta l'usuari root com a usuari SAMBA. Un consell per mantenir la seguretat: si bé és necessari l'usuari root per donar d'alta els clients de xarxa no cal que estigui "sempre" actiu. Una interessant forma de fer-ho és donar-lo d'alta "únicament" durant el procés d'alta dels clients i després esborrar-lo. També és important que no s'usi la mateixa paraula clau per l'usuari root de SAMBA que el que s'ha usat com a paraula clau de l'usuari administrador de Linux. Per donar d'alta l'usuari root des de la línia de comandes cal fer:

```
estacio-1:/ # smbpasswd -a root
New SMB password:
Retype new SMB password:
Added user root.
estacio-1:/ #
```

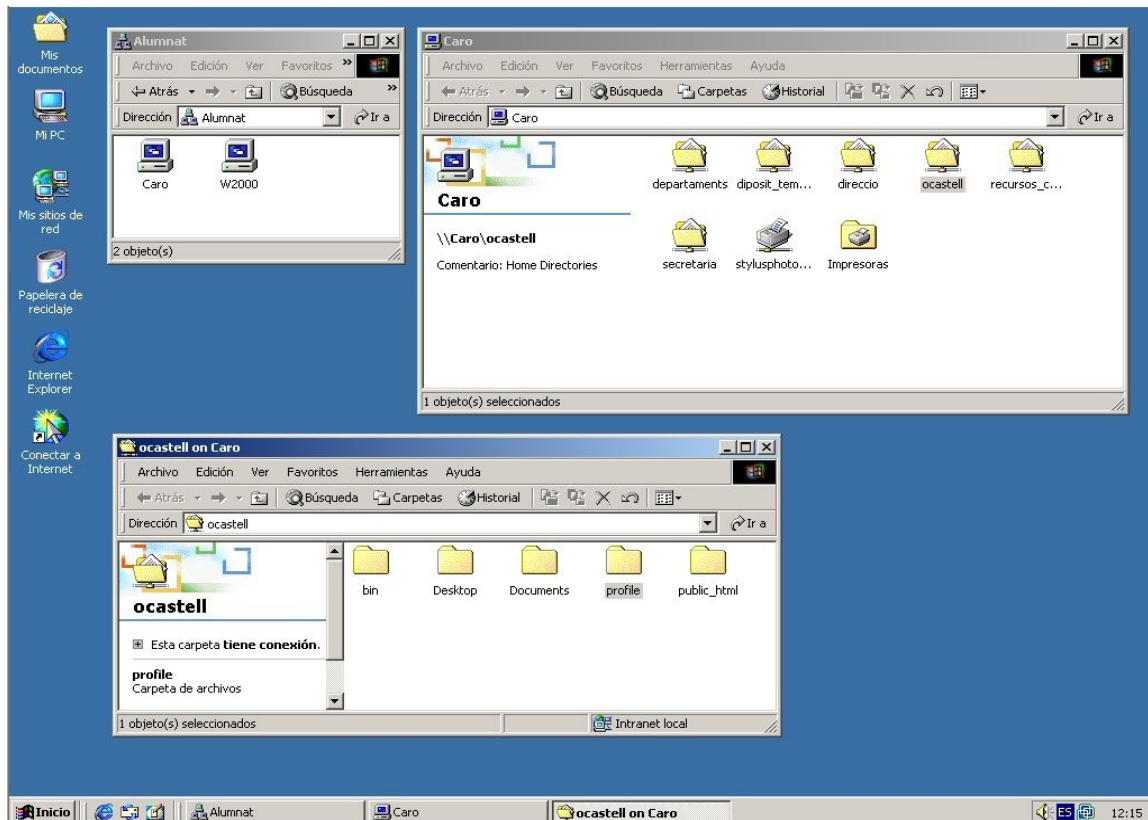
Així, per un client Windows tindrem el següent:



El sistema Windows (com sempre) ens demanarà reiniciar el sistema. Una vegada s'ha tornat a engegar, veurem que la pantalla d'inici de Windows ha canviat i que ens demana un usuari i una paraula clau i la connexió a un domini (**alumnat**) o a la màquina local. Si intentem validar un usuari de la xarxa (que estigui donat d'alta al servidor Linux) però escollim el domini de la màquina local ens serà impossible entrar al sistema. Si escollim entrar al domini **alumnat** amb un usuari que s'hagi donat d'alta no tindrem cap problema. La primera vegada que entrarà l'usuari es crearà el seu perfil que es guardarà al servidor una vegada es desconnecti conservant tota la seva configuració personal en la carpeta **profile** de la seva zona d'usuari del servidor. Aquest serà a partir d'ara el seu perfil de xarxa. Una pràctica interessant és veure com es conserva la configuració de l'escriptori Windows d'un usuari validat en la xarxa d'un client a un altre.



Per veure els recursos compartits del servidor tenim dues possibilitats. Ho podem fer navegant per l'entorn de la xarxa fins arribar al servidor i veure les carpetes que ofereix:



També podem utilitzar la funcionalitat del *Netlogon* on s'ha ubicat un fitxer *XARXA.BAT* d'execució per tots els usuaris validats. Això vol dir que en validar-se un usuari a la xarxa, el client Windows executa un fitxer BAT amb una sèrie de comandes DOS que permeten (per exemple) connectar unitats de xarxa a recursos compartits. Això mateix es pot utilitzar per comunicar notícies als usuaris amb una petita modificació del *XARXA.BAT*. Mirem el contingut del fitxer en qüestió:

```
@ECHO OFF
@ECHO Intentant assignar les lletres X:, Y:, T: a la xarxa ...

IF EXIST Y:\CON NET USE Y: /delete /YES
NET USE Y: \\caro\Recursos_Centre /YES

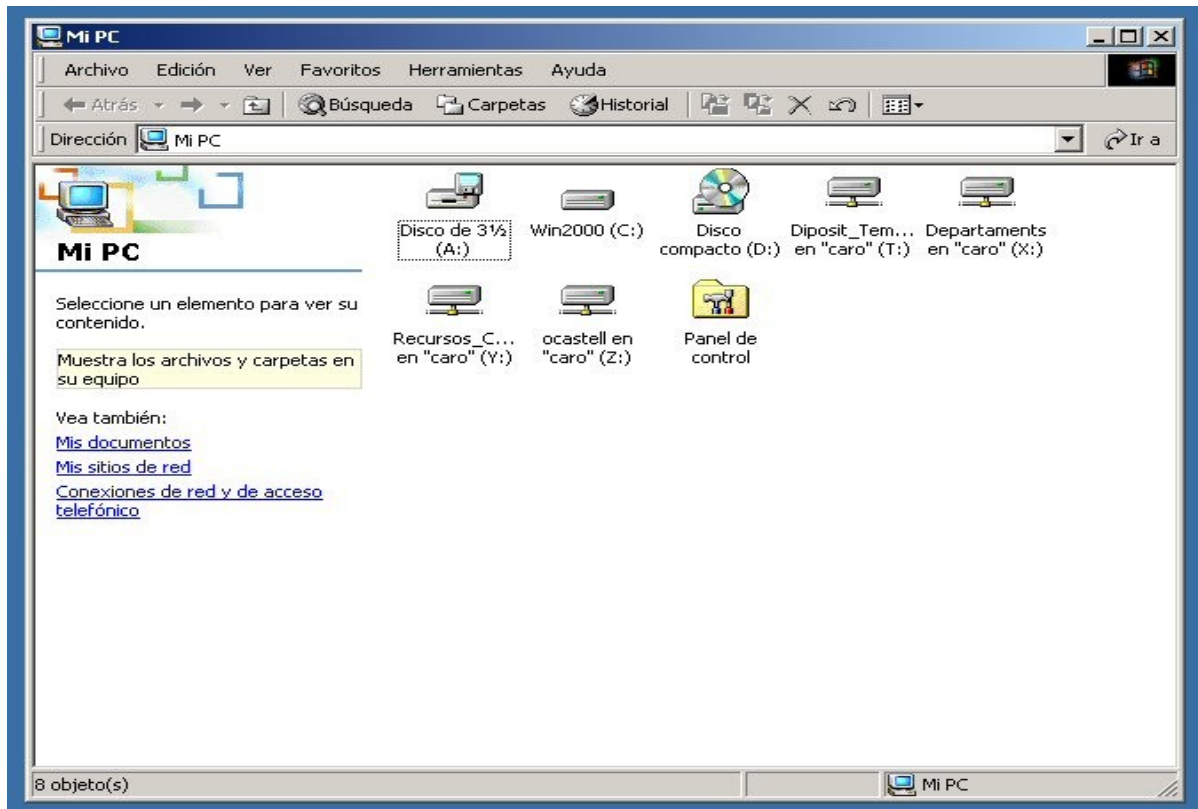
IF EXIST X:\CON NET USE X: /delete /YES
NET USE X: \\caro\Departaments /YES

IF EXIST T:\CON NET USE T: /delete /YES
NET USE T: \\caro\Diposit_Temporal /YES

NET TIME \\caro /SET /YES
```

Es connecten les unitats de xarxa Y: (a Recursos_Centre), X: (a Departaments) i T: (a Diposit). A més a més, es sincronitza el temps del sistema amb el temps del servidor que s'ha configurat com un servidor de temps. Aquest fitxer BAT de connexió general es pot particularitzar per un usuari o grup del domini, tal com indica el manual de SAMBA, de manera que podem escollir què es connecta a segons quins usuaris o grups.

L'efecte de l'execució de l'anterior fitxer en un client Windows és que en Mi PC apareixen unes noves unitats assignades a recursos de la xarxa, tal com es pot veure en la següent figura, de manera que en fer un clic a sobre anem directament al recurs corresponent sense haver de navegar.



La configuració d'un client SAMBA en un ordinador amb sistema Linux és una mica més senzilla. Primer que res cal repassar la configuració TCP/IP de la targeta de xarxa. Cal que sigui idèntica a la configuració que hem fet per els clients Windows. Una vegada la configuració TCP/IP és la correcta la configuració d'un client SAMBA amb Linux és fa modificant sensiblement el fitxer `smb.conf` del client Linux. Ho podem fer, com abans, en línia de comandes, utilitzant WEBMIN o per mig de YAST (en el cas de SuSE). El fitxer de configuració de la secció [global] d'un client SAMBA en Linux quedaria així:

```
[global]
workgroup = alumnat
netbios name = estacio-1
username map = /etc/samba/smbusers
map to guest = Bad User
security = user
encrypt passwords = yes
```

SuSE (en la versió de finestres KDE) incorpora un navegador per la xarxa local molt similar al que incorpora Windows (molt més potent ja que permet altres protocols addicionals a CIFS com ara SSH, FTP ...). El navegador està integrat en **konqueror**. Encara així, pel que ens interessa que és accedir als recursos compartits del servidor, la manera fàcil de fer-ho és escriure el següent al navegador:

smb:/ocastell@caro/ocastell

Per exemple, per accedir a la zona d'usuari d'ocastell al servidor com usuari identificat. Ens demanarà la paraula clau per entrar al recurs compartit. Cal ficar la corresponent a l'usuari, el qual ha d'estar donat d'alta del servidor SAMBA principal.

3.3.2 Paràmetres de xarxa i altes massives d'usuaris

Configurat el nostre servidor SAMBA principal ens queda discutir sobre la configuració dels dos servidors restants (gestió i professorat) i veurem com fem complir els requisits de seguretat que s'han plantejat al projecte. La configuració d'aquest dos servidors serà pràcticament la mateixa amb dues diferències importants:

1. Les interfícies de xarxa on SAMBA transmet el seus paquets. És a dir els trams IP.
2. Els usuaris que formaran part de cada domini.

El servidor SAMBA, per defecte, està configurat per enviar i escoltar el tràfic de xarxa de totes les interfícies de xarxa del sistema. Així, en el nostre cas anterior, el servidor principal transmet i rep els paquets d'informació per tots els trams IP definits al servidor, el que significa que les aules poden accedir als recursos compartits però també ho poden fer els ordinadors de les dependències de gestió i professorat. Per un altra banda, no ens interessa que passi el mateix però a la inversa, és a dir, que els ordinadors de les aules puguin accedir als recursos compartits dels servidors i dominis de gestió i professorat. El fet d'estar en xarxes separades ja és per si mateix un primer nivell per assegurar aquest fet però, podem augmentar el nivell de seguretat indicant als serveis SAMBA configurats als servidors de gestió i professorat que únicament enviïn i rebin tràfic de xarxa per un tram de xarxa determinat.

El paràmetre que ens permet fer això és `INTERFACES` de la secció `[global]` i que ha de representar la IP de la targeta de xarxa i la màscara de la xarxa on volem transmetre. Així, per als servidors de gestió i professorat seran respectivament:

```
S-GESTIO -----> INTERFACE = 192.168.0.2/255.255.255.0
S-PROFESSORAT----> INTERFACE = 192.168.0.3/255.255.255.0
```

L'altra part important de la seguretat que introduïm en el sistema d'aquesta xarxa són els permisos corresponents als usuaris i grups. Primer que res cal entendre que els usuaris estan repartits en tots tres servidors, de manera que:

1. Els usuaris del domini de gestió estan donats d'alta amb el mateix nom i pertanyen al mateix grup a tots tres servidors. Els seus permisos, per tant, són idèntics en tots tres dominis.
2. Els professors estan donats d'alta i pertanyen al mateix grup en els servidors d'alumnat i professorat, conservant els seus permisos a tots dos servidors.
3. Els alumnes únicament estan donats d'alta al servidor de l'alumnat.

Aquesta distribució jeràrquica dels usuaris representa un esforç afegit al moment de donar d'alta els usuaris al sistema. Cal seguir una política molt estricta d'assignació de grups i d'assignació de permisos a cada grup i/o usuari. Una eina que ens pot ajudar a donar d'alta els usuaris d'una manera coherent, controlada i sense un gran esforç és sense dubte `WEBMIN`.

L'aplicatiu disposa d'un sistema per realitzar altes massives d'usuaris a partir d'un fitxer de text amb un format determinat on, línia a línia, es dona la informació necessària per crear un usuari al sistema. Recordem que ja varem ficar al fitxer de configuració de SAMBA que qualsevol usuari que es doni d'alta al sistema seria automàticament un usuari de SAMBA. La informació que cal donar és la que segueix i amb el següent format:

```
create:usuari:ctsenya:uid:gid:nomreal:dirarrel:shell:min:max:avis:inactiu:expira
modify:vellusuari:usuari:ctsenya:uid:gid:nomreal:dirarrel:shell:min:max:avis:inactiu:expira
delete:vellusuari
```

La primera paraula és una clau per crear, modificar o esborrar l'usuari. La resta de paraules són:

<i>Paraula</i>	<i>Descripció</i>
usuari	Fa referència al nom d'usuari al sistema (i per tant a SAMBA) – Obligatori-
vellusuari	És el nom d'un usuari ja existent al sistema -Obligatori en <i>modify</i> i <i>delete</i> -
ctsenya	És la paraula clau de l'usuari -Opcional-
uid	És el número d'identificació de l'usuari -Opcional- Defecte: assignat pel sistema.
gid	És el número d'identificació del grup al que pertany l'usuari -Opcional- Defecte: assignat pel sistema.
nomreal	És el nom real de l'usuari (informació) -Opcional-
dirarrell	És el directori que es crea per l'usuari -Opcional- Defecte: assignat pel sistema.
shell	és la shell script assignada a l'usuari -Opcional- Defecte: assignat pel sistema.
min	Període de temps mínim en dies de validesa de la paraula clau de l'usuari -Opcional- Defecte: assignat pel sistema.
max	Període de temps màxim en dies de validesa de la paraula clau de l'usuari -Opcional- Defecte: assignat pel sistema.
avis	Període de temps en dies que s'avisava l'usuari per canviar la seva paraula clau -Opcional- Defecte: assignat pel sistema.
inactiu	Nombre de dies d'inactivitat de l'usuari a partir dels que el sistema el convertirà en un usuari inactiu -Opcional- Defecte: assignat pel sistema.
expira	Data en que l'usuari serà donat de baixa del sistema o estarà inactiu -Opcional- Defecte: assignat pel sistema.

Podem generar el fitxer de text amb la informació a partir d'una base de dades on estiguin els noms i cognoms dels usuaris a crear utilitzant, per exemple, qualsevol full de càlcul a la nostra disposició.

Un cop s'ha generat el fitxer de text es creen els usuaris amb WEBMIN: cal anar a *Sistema -> Usuaris i Grups -> Crea, modifica i suprimeix usuaris des d'un fitxer batch*. Tenim l'opció de pujar el fitxer o d'utilitzar un fitxer local del servidor. També ens dona diverses opcions, com crear i/o modificar l'usuari a altres mòduls (molt important al nostre cas que sigui que sí) i altres.

Com a pràctica del mòdul seria interessant generar un fitxer amb tots els assistents al curs i donar-los d'alta al servidor que cadascun està treballant. Una vegada fet, cal visualitzar el contingut dels fitxers */etc/passwd* i */etc/samba/smbpasswd* per veure que és el que ha passat.

Com a proposta de pràctica al taller farem les següents activitats:

Instal·lació i configuració d'un servidor SAMBA:

Cada un dels assistents al curs en el seu servidor de pràctiques instal·larà i configurarà un servei SAMBA:

- ✓ Primer caldrà determinar el tram IP i configurar la xarxa (evitant repeticions amb la resta d'assistents).
- ✓ Caldrà decidir un nom propi i únic per al domini i el servidor.
- ✓ Es crearan usuaris manualment. A ser possible es faran pràctiques per incloure clients WINDOWS i Linux al domini SAMBA.
- ✓ Es farà la creació d'usuaris massiva utilitzant una base de dades dels assistents al curs.
- ✓ Una vegada creats els usuaris i grups es faran diferents pràctiques d'assignació de permisos a nivell SAMBA i Linux per als recursos compartits.

Perfils mòbils:

Podem comprovar el funcionament dels perfils mòbils utilitzant un dels usuaris creats i alguns dels clients windows que s'hagin introduït al domini:

- ✓ Ens validarem amb un usuari de xarxa en un dels clients.
- ✓ Farem modificacions a l'escriptori: creació de documents, canvi del fons de pantalla, creació d'icones i enllaços.
- ✓ Desconnectarem l'usuari d'aquest client i anirem a un client diferent per validar-lo: observem què passa amb l'entorn de l'usuari.
- ✓ Mirem què hi ha al servidor SAMBA. Anirem al servidor Linux i mirarem el contingut del directori *profile* de la carpeta de l'usuari que s'ha utilitzat en la pràctica.
- ✓ Com a root esborrem el contingut de la carpeta *profile* i tornem a fer les proves.

Creació de fitxers BAT:

Per veure el funcionament dels fitxers BAT podem crear scripts a mida per cada un dels servidors. Això es pot fer des de Linux però també des dels clients windows si donem els permisos correctes al directori *netlogon* i el seu contingut:

- ✓ Localitzem el directori *netlogon* al servidor Linux i donem permisos a un usuari de xarxa perquè el pugui modificar.
- ✓ Creem un fitxer XARXA.BAT senzill.
- ✓ Des d'un client windows comprovem el funcionament.
- ✓ Des del client windows, amb l'usuari escollit abans, modifiquem el fitxer XARXA.BAT amb el Bloc de Notes de windows
- ✓ Creem fitxers BAT per usuaris particulars.

Referències:

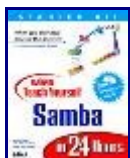
[1] Projecte SAMBA. Web Oficial: <http://www.samba.org>

[2] Projecte LDAP. Web Oficial: <http://www.openldap.org>

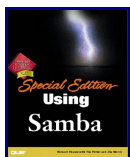
[3] Llibres sobre SAMBA:



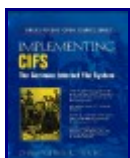
John Blair, [Samba: Integrating UNIX and Windows](#).



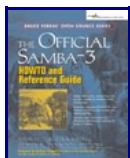
Jerry Carter and Richard Sharpe, [SAMS Teach Yourself Samba in 24 Hours](#).



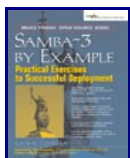
Richard Sharpe and Tim Potter, [Special Edition, Using Samba](#).



Chris Hertel, [Implementing CIFS](#),



John H. Terpstra and Jelmer R. Vernooij, [The Official Samba-3 HOWTO and Reference Guide](#).



John H. Terpstra *The Official Samba-3 HOWTO and Reference Guide*.

[4] Comparativa Windows/Linux:

Seguretat <http://www.zone-h.org/en/winvslinux2>

Prestacions: <http://www.anedonia.net/gnulinix-vs-windows/>

<http://bulma.net/body.phtml?nIdNoticia=1035>