Linux Meeting Nov 2003, Samba Intro

Alain Knaff
alain.knaff@linux.lu

Summary

- 1. Basic config (defining shares, ...)
- 2. Operating as a PDC
- 3. Password synchronization
- 4. Access control
- 5. Samba variables
- 6. Advanced printing
- 7. Misc gimmicks

Basic config (smb.conf)

- Sections, intoduced by [*sectionName*]
- Global section: settings apply to all shares
- Share section: settings apply to this share
- Reserved sections/shares: `printers`, `netlogon`, ...
- User management

Basic config. Global parameters

- workgroup
- printing
  - plp
  - lprng
  - cups
  - ...
- security
  - user
  - domain
  - share

Basic config. Share specific parameters

- comment
- browseable
- public
- read only
- available

Basic config. File Share

- `path`

Basic config. Printer share

- `printable = yes`
- `printer = hp4550`
- `path`

Basic config. General Printers share

- `load printers = yes`
- `[printers]`

Basic config. User management

- `encrypt password = yes`
- different passwords db for Unix and Windows clients:
  `/etc/samba/smbpasswd` file
- Add a Windows user: `smbpasswd -a`
- `guest user = nobody`
- map Windows users to Unix users:
  `username map = /etc/samba/user.map`
- Username map example:

```
root = admin administrator
tridge = "Andrew Tridgell"
```

Basic config. Testing

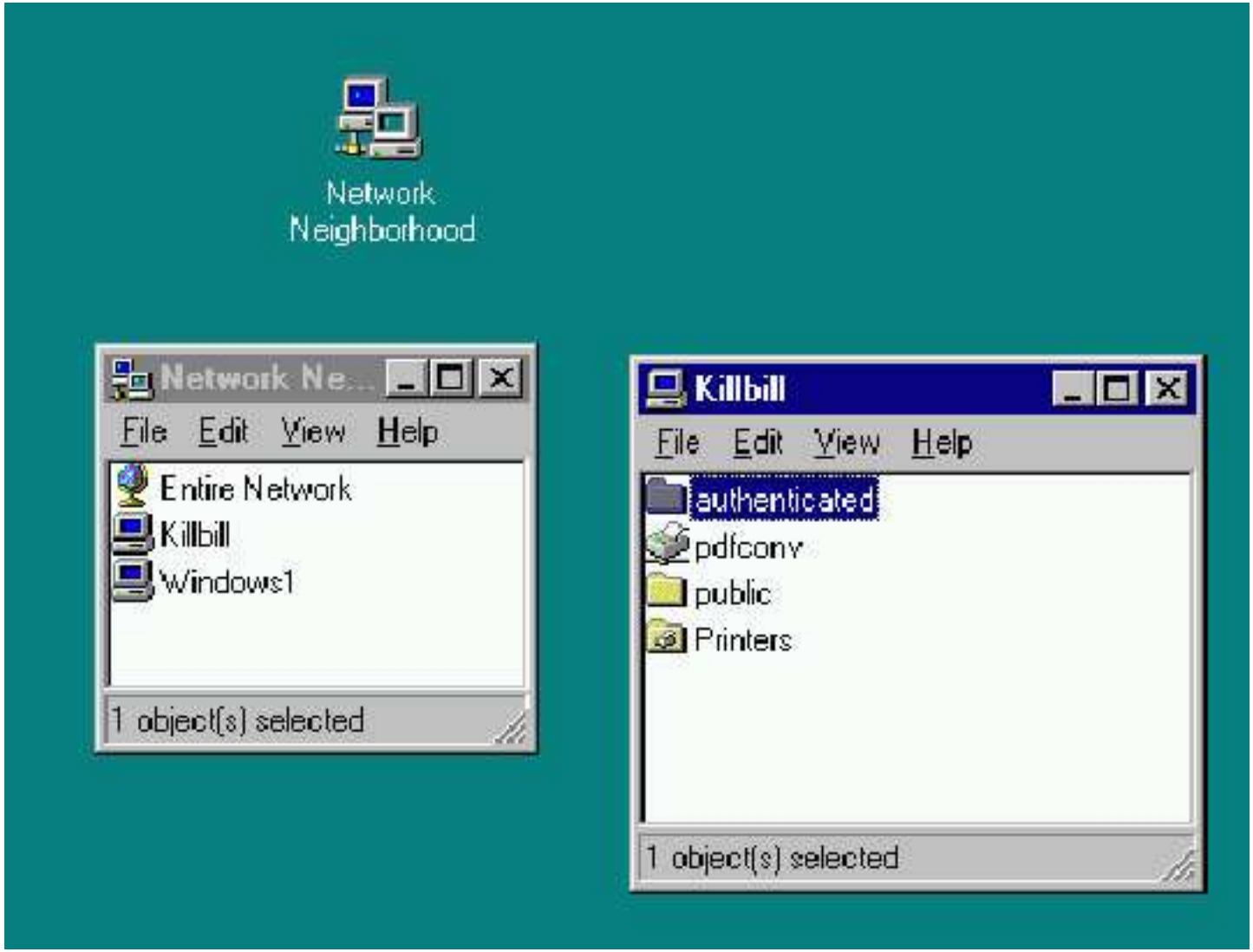
- `testparm`
- `smbclient //server/share -U user`

Basic config. Example

```
[global]
        workgroup = test
        printing = lprng
        load printers = yes
        encrypt passwords = yes
[public]
        comment = A Test Share
        browseable = yes
        public = yes
        read only = yes
        path = /samba/public
[authenticated]
        comment = An authenticated share
        browseable = yes
        read only = no
        path = /samba/auth

[printers]
        comment = Printers share
        printable = yes
```

Basic config. Windows screenshot



Primary domain controller

- Global settings
- Netlogon share
- Profile directory

PDC: global settings

- Enable PDC: `domain logons = yes`
- Security: `security = user`
- Workgroup parameter is interpreted as domain
- Set up as wins server: `wins support = yes`
- Set up domain administrator: `domain admin group = root`
- Script for creating machine accounts:

```
add user script = /usr/sbin/useradd -d / -g 100 -s /bin/false -M %u
```

- Drive letter for home directory: `logon drive = "H:"`
- Home directory share: `[homes]`

PDC: startup script

- Define a netlogon share
- `logon script = "STARTUP.BAT"`

PDC: profile storage

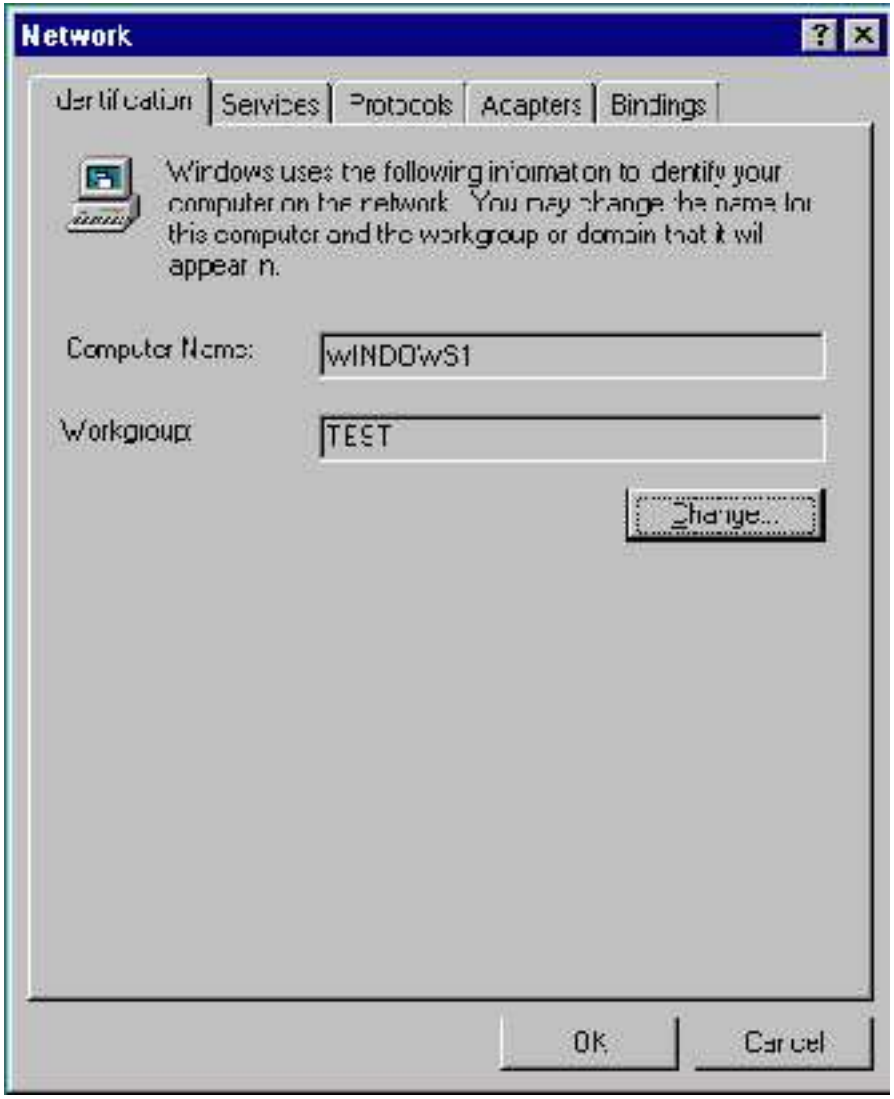
- Windows 95/98: `logon home`
- Windows NT/2000/XP: `logon path`

PDC: example

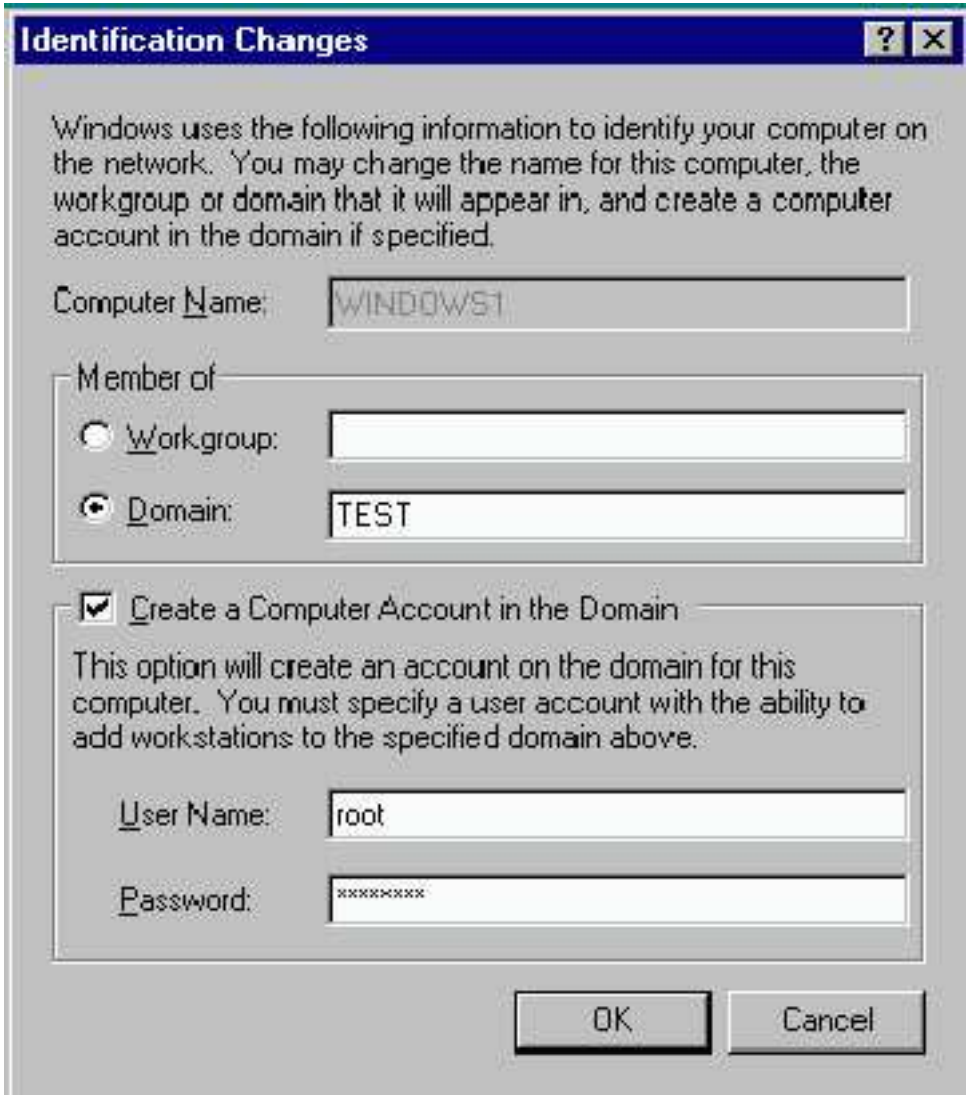
```
[global]
        workgroup = test
        printing = lprng
        load printers = yes
        username map = /etc/samba/user.map
        encrypt passwords = yes

        wins support = yes
        domain logons = yes
        domain admin group = root
        add user script = /usr/sbin/useradd -d / -g 100 -s /bin/false -M %u
[homes]
        comment = Home Directory Share
        read only = no
…
```

PDC: setting up the client



PDC: setting up the client



PDC: setting up the client (XP)

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters]
"requiresignorseal"=dword:00000000
```

Password synchronization

- Global settings
- Unix pass follows windows: `/etc/pam.d/samba`
- Windows pass follows Unix: `/etc/pam.d/passwd`

Password synchro: global settings

- `unix password sync = Yes`
- `pam password change = Yes`

Password synchro: /etc/pam.d/samba

```
auth     required   pam_unix.so
account  required   pam_unix.so
password required   pam_pwcheck.so  nullok
password required   pam_unix2.so    nullok use_first_pass use_authtok
```

Password synchro: /etc/pam.d/passwd

```
auth     required  pam_unix2.so    nullok
account  required  pam_unix2.so
password required  pam_pwcheck.so  nullok
password required  pam_unix2.so    nullok use_first_pass use_authtok
password required  pam_smbpass.so  nullok try_first_pass use_authtok
session  required  pam_unix2.so
```

Access control

- By user
- By IP
- Controlling Unix rights once access is granted

Access control: by user

- Users who can/cannot access:
  - `valid users`
  - `invalid users`
  - invalid users takes precedence
- Users who can/cannot write:
  - `write list`
  - `read list`
  - write list takes precedece
- Allmighty users:
  - `admin users`

Access control: by ip

- `hosts deny`
- `hosts allow`
- allow takes precedence

Access control: unix rights

- User/group
  - `force user`
  - `force group`
- Permission bits on creation
  - maximal [AND]: `(directory|create) mask`
  - minimal [OR]: `force (directory|create) mode`
- Permission bits for chmod
  - `[directory] security mask`
  - `force [directory] security mode`
- Write access implies chmod access:
  - `dos filemode = yes`

Samba variables

- `%U` user name requested
- `%u` user name granted (after force)
- `%G` primary group of `%U`
- `%g` primary group of `%u`
- `%H` home directory of `%u`
- `%m` NetBIOS name of client machine
- `%I` IP of client
- `%a` Win variant of client (WfWg, Win95, WinNT, Win2k, ...)
- `%L` name of the server

- Example:

```
logon path = \\%L\%U\profile.%a
```

User monitoring/logging

- `smbstatus` displays currently active sessions
- Account samba sessions in wtmp (last):
  - `root preexec = /usr/X11R6/bin/sessreg -l %m -h %M -a %u`
  - `root postexec = /usr/X11R6/bin/sessreg -l %m -h %M -d %u`

Advanced printer support

- `add printer command`: script to add a printer to printcap
- `enumports command`: script listing all current printers
- `postscript = yes`: add %! to start of print output to avoid printer confusion by bad clients
- `printer admin = joe`: adds joe as administrator for printer share
- `show add printer wizard = yes`

Other gimmicks

- Time service
- Veto/hide files
- Include/override config files

Others: time service

- In global config: `time server = yes`
- On client (or startup script): `net time \\server /set`

Others: hiding files

- In share config
- Hides files (by setting hidden bit): `hide files = *.exe/*.scr`
- Hides files completely: `veto files = *.exe/*.scr`

Others: include/override config

- Override:
  - `config file = /usr/local/samba/lib/smb.conf.%m`
  - replaces current config
  - ignored if file does not exist
- Include:
  - `include = /usr/local/samba/lib/smb.conf.%m`
  - supplements current config
  - ignored if file does not exist (TBC)

Online configuration tool:

- SWAT

URL of this presentation

- This presentation will be placed at the following address

`http://www.lll.lu/Presentations/samba-2003-11-27/samba.pdf`