Implementasi Samba PDC menggunakan backend LDAP

Ratdhian Cipta Sukmana
ratdix@yahoo.com
http://ratdix.wordpress.com

Pendahuluan

Artikel ini merupakan materi lanjutan dari artikel tentang LDAP yang telah Penulis tulis sebelumnya. Untuk itu silahkan Anda membaca artikel Pengenalan LDAP agar lebih memudahkan pemahaman Anda tentang LDAP yang pada artikel ini akan di jadikan backend untuk Samba PDC.

Samba dibuat dan di susun pertama kali oleh *Andrew Tridgell*, yang sekarang masih mengepalai pengembangan Samba dari rumahnya di *canberra (Austrlia)* bersama para *Samba Development Team* yang tersebar di seluruh dunia. Project Samba ini lahir pada tahun 1991 ketika Andrew berhasil meng-copy file mesin PATHWORK dari *Digital Equipment Corporation* ke dalam jaringan lokalnya. Beberapa tahun kemudian Andrew mulai mendistribusikan ke internet menggunakan nama *SMB SERVER*, akan tetapi karena nama ini telah di gunakan maka ia-pun mencari nama baru menggunakan pendekatan unik dengan cara :

*grep –i 's.*m.*b' /usr/dict/words*

dan hasilnya adalah

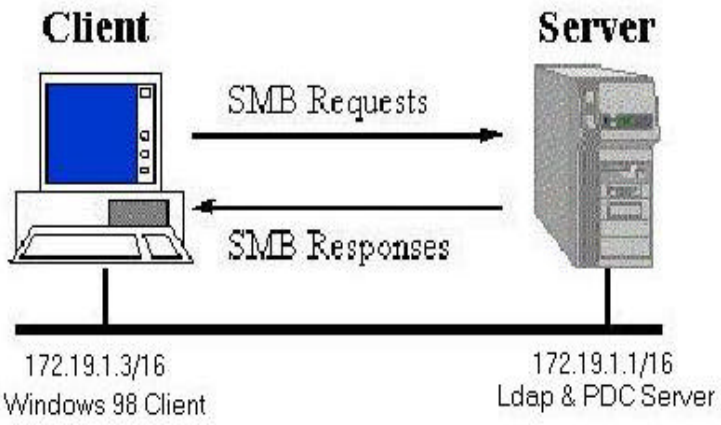
salmonberry samba sawtimber scramble

Maka terpilihlah dan lahirlah nama *Samba* untuk program kecil yang luar biasa ini.

Konsep dasar

Samba merupakan suatu aplikasi unix yang menyembatani komunikasi dengan mesin lain menggunakan protokol *SMB (Server Message Block).* Jadi sebelum Penulis menjelaskan Samba lebih lanjut, Penulis akan menjelaskan fungsi beberapa protokol yang di gunakan oleh Samba.

SMB (Server Message Block) merupakan sebuah protokol yang di gunakan untuk berbagi file, printer, serial port dan lainnya agar dapat di gunakan secara bersama pada komputer yang terhubung ke jaringan. *SMB* juga menggunakan konsep *Client-Server*, dimana client menghubungi *(Request)* server menggunakan *TCP/IP*, *NetBEUI* atau *IPX/SPX*. Apabila koneksi ini berhasil maka client akan mengirimkan *Command SMBs* ke server yang akan mengizinkan mereka untuk menggunakan file, printer atau *resource* yang di *share.* Bila *SMB* dipakai bersama *TCP/IP* atau *NetBEUI*, maka penggunaan N*etBIOS Names* untuk beberapa kasus mutlak di perlukan. Saat sebuah



Gambar 1

komputer dalam jaringan di aktifkan, maka mesin tersebut akan mengirimkan pesan secara *broadcast* (kepada seluruh komputer yang ada dalam jaringan) dan mendeklarasikan dirinya dengan nama dari *NetBIOS*, sehingga *NetBIOS*-lah yang memetakan mesin tersebut menjadi suatu nama. Dan pada saat mendeklarasikan namanya dalam sebuah jaringan, mesin juga melayani *name resolution* yang merupakan sebuah proses penerjemahan nama *NetBIOS* ke dalam nomor *IP* tertentu.

Dalam membangun SMB Server, Anda harus memahami perbedaan istilah *Workgroup* dan *Domain*. *Workgroup* merupakan kumpulan dari beberapa komputer yang mengatur sekuritas sumber dayanya masing-masing, sehingga tingkat keamanan dalam jaringan workgroup terdistribusi. Sedangkan *Domain* merupakan kumpulan dari beberapa komputer yang mengatur sekuritas dan sumber daya terpusat, sehingga tingkat keamanannya tersentral pada suatu mesin. Mesin yang mengontrol sekuritas pada Domain di namakan *PDC (Primary Domain Controller)* dan mesin yang mengambil alih tugas *PDC* ketika mengalami *crash* di sebut *BDC (Backup DomainController).* Secara periodik mesin *PDC* dan *BDC* akan melakukan sinkronisasi *SAM (Security Account Manager).* Sedangkan *SAM* sendiri biasanya merupakan suatu data yang menyimpan daftar *username* dan *password*.

Lalu apa yang dapat Kita lakukan dengan Samba…….?

Pertanyaan seperti di atas mungkin akan muncul di benak Anda dan penjelasan yang termudah yaitu bahwa :

- Samba dapat membantu mesin Windows atau OS2 dan unix untuk berkomunikasi dalam suatu network
- Samba menjadikan mesin unix Anda dapat berbagi (share) file, printer dan dengan melakukan konfigurasi yang tepat maka samba dapat di jadikan *file & print server*
- Samba bisa di jadikan mesin *PDC* atau *BDC* yang dapat memberikan otentikasi kepada tiap client yang login ke dalam Domain. Samba-pun dapat di jadikan member dari suatu Domain.
- Samba dapat di jadikan *WINS* server yang dapat menyimpan daftar nama *NetBIOS* dalam jaringan.
- Samba dapat membantu pengguna melakukan browsing di *network neighborhood*

Samba biasanya di sertakan dalam tiap distribusi Linux dan merupakan kumpulan aplikasi yang bergantung satu sama lain. Samba sendiri memiliki dua buah *daemon* yaitu :

smbd

Merupakan daemon yang memberikan layanan berbagi file dan printer di dalam SMB Network dan menyediakan layanan otentikasi dan autorisasi bagi SMB Client

nmbd

Merupakan Daemon yang memanfaatkan Windows Internet Name Service (WINS) dan melayani permintaan name server lalu akan memberikan respon yang sesuai.

Instalasi dan Konfigurasi Samba sebagai PDC

Penulis berusaha menerangkan konsep dasar dalam penulisan konfigurasi PDC, dengan maksud memudahkan Anda dalam memahami samba dan ldap, apabila Anda telah memahami samba dan konfigurasinya dengan baik, Anda dapat lakukan konfigurasi yang lebih optimal dan aman.

Pastikan paket samba telah terinstal dengan baik

```
[root@ldap ~]# rpm -qa |grep samba
samba-common-3.0.14a-2
samba-3.0.14a-2
system-config-samba-1.2.31-1
samba-client-3.0.14a-2
```

Buka konfigurasi smb.conf, dan konfigurasikan seperti berikut :

[root@ldap ~]# vim /etc/samba/smb.conf

```
------------------------------ smb.conf ----------------------------------
[global]
workgroup = SMARTBEE
netbios name = LDAP
security = user
os level = 80
local master = yes
domain master = yes
preferred master = yes
domain logons = yes
wins support = yes
logon script = %U.bat

[netlogon]
   comment = Network Logon Service
   path = /home/netlogon
   guest ok = yes
   writable = no
   share modes = no
[Profiles]
    path = /home/profiles
    browseable = no
    guest ok = yes
------------------------------ end of smb.conf ----------------------------------
```

Buatlah direktori netlogon dan profile berserta permission-nya

[root@ldap ~]# mkdir -m 0775 /home/netlogon
[root@ldap ~]# mkdir /home/profiles
[root@ldap ~]# chmod 1757 /home/profiles

Lakukan test konfigurasi samba yang telah Anda buat

[root@ldap ~]# testparm
```
Load smb config files from /etc/samba/smb.conf
Processing section "[netlogon]"
Processing section "[Profiles]"
Loaded services file OK.
Server role: ROLE_DOMAIN_PDC
Press enter to see a dump of your service definitions
```

Selamat, PDC server Anda telah terinstall…….

Instalasi dan Konfigurasi Samba LDAP tools

Untuk mengimplementasikan samba menggunakan LDAP Backend, Anda membutuhkan paket smbldap-tools, sedangkan peket ini membutuhkan beberapa dependensis yang harus Anda instal terlebih dahulu diantranya :
perl(Digest::MD4), perl(Digest::MD4), perl(Jcode) is needed, perl(Unicode::Map), perl(Unicode::Map), perl(Unicode::Map), perl(Unicode::Map), smbldap-tools

Semua paket-paket tersebut dapat Anda download pada :
ftp://fr2.rpmfind.net/linux/fedora/extras/4/i386

Sedangkan paket *perl(Digest::SHA1)* dapat Anda dapatkan di cd pertama Fedora core 4

install smbldap-tools lalu lakukan langkah-langkah berikut :

[root@ldap ~]# rpm -ivh /package/download/smbldap-tools-0.9.2-2.fc4.noarch.rpm
[root@ldap ~]# cp /usr/share/doc/samba-3.0.14a/LDAP/samba.schema /etc/openldap/schema/

Edit file slapd.conf dan tambahkan baris berikut …

---------- add script on slapd.conf ----------
```
include /etc/openldap/schema/samba.schema
index sambaSID                  eq
index sambaPrimaryGroupSID      eq
index sambaDomainName           eq
index default                   sub
```

Edit file smb.conf dan tambahkan baris berikut di direktori global

---------- add script on smb.conf ----------
```
passdb backend = ldapsam:ldap://localhost
add user script = /usr/sbin/smbldap-useradd -m '%u'
delete user script = /usr/sbin/smbldap-userdel '%u'
add group script = /usr/sbin/smbldap-groupadd '%g'
delete group script = /usr/sbin/smbldap-groupdel '%g'
add user to group script = /usr/sbin/smbldap-groupmod -m '%u' '%g'
delete user from group script = /usr/sbin/smbldap-groupmod -x '%u' '%g'
set primary group script = /usr/sbin/smbldap-usermod -g '%g' '%u'
add machine script = /usr/sbin/smbldap-useradd -w '%u'

ldap admin dn = cn=manager,dc=smartbee,dc=com
ldap group suffix = ou=Groups
ldap machine suffix = ou=hosts
```

```
ldap passwd sync = Yes
ldap suffix = dc=smartbee,dc=com
ldap ssl = no
ldap timeout = 20
idmap backend = ldap:ldap://localhost
   idmap uid = 15000-20000
   idmap gid = 15000-20000
ldap user suffix = ou=People
winbind nested groups = No
ea support = Yes
map acl inherit = Yes
```

Dapatkan lokalSID dan masukkan nilainya kedalam smbldap.conf dan lanjutkan sbb :

[root@ldap ~]# net getlocalsid
SID for domain LDAP is: S-1-5-21-2835300851-3378749978-4166134816
[root@ldap ~]# vim /etc/smbldap-tools/smbldap.conf

---------- smbldap.conf ----------

```
SID="S-1-5-21-2835300851-3378749978-4166134816"
sambaDomain="SMARTBEE"
suffix="dc=smartbee,dc=com"
usersdn="ou=People,${suffix}"
computersdn="ou=Hosts,${suffix}"
groupsdn="ou=Group,${suffix}"
idmapdn="ou=Idmap,${suffix}"
sambaUnixIdPooldn="sambaDomainName=SMARTBEE,${suffix}"
scope="sub"
hash_encrypt="CLEARTEXT"
userLoginShell="/bin/bash"
userHome="/home/%U"
userHomeDirectoryMode="700"
userGecos="System User"
defaultUserGid="513"
defaultComputerGid="515"
skeletonDir="/etc/skel"
defaultMaxPasswordAge="45"
userSmbHome="\\LDAP\%U"
userProfile="\\LDAP\profiles\%U"
userHomeDrive="P:"
userScript="%U.bat"
mailDomain="smartbee.com"
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
with_slappasswd="0"
```

```
slappasswd="/usr/sbin/slappasswd"
---------------------------------- end of smbldap.conf ----------------------------------
```

[root@ldap ~]# vim /etc/smbldap-tools/smbldap_bind.conf

```
------------------------------------ smbldap_bind.conf ------------------------------------
slaveDN="cn=Manager,dc=smartbee,dc=com"
slavePw="rahasia"
masterDN="cn=Manager,dc=smartbee,dc=com"
masterPw="rahasia"
---------------------------------- end of smbldap_bind.conf ----------------------------------
```

Jalankan Samba dan masukkan password root ke dalam database sebagai berikut :

```
[root@ldap ~]# /etc/init.d/smb start
Starting SMB services:                     [  OK  ]
Starting NMB services:                     [  OK  ]
[root@ldap ~]# smbpasswd -w rahasia
Setting stored password for "" in secrets.tdb
```

Agar memudahkan Anda dalam memahami perbedaan konfigurasi pada materi *Pengenalan LDAP* Penulis sarankan Anda membuat file LDIF baru dan menghapus data pada ldap sebelumnya, sebagai berikut :

```
[root@ldap ~]# /etc/init.d/ldap stop
[root@ldap ~]# vim smbldap.ldif
------------------------------------ smbldap.ldif ------------------------------------
dn: dc=smartbee,dc=com
objectClass: dcObject
objectClass: organization
o: smartbee
dc: smartbee

dn: ou=people,dc=smartbee,dc=com
objectClass: organizationalUnit
ou: people
description: User List

dn: ou=Idmap,dc=smartbee,dc=com
objectClass: organizationalUnit
ou: Idmap
description: User List

dn: ou=groups,dc=smartbee,dc=com
objectClass: organizationalUnit
```

ou: groups
description: Group List

dn: sambaDomainName=SMARTBEE,dc=smartbee,dc=com
objectClass: sambaDomain
sambaDomainName: SMARTBEE
sambaSID: S-1-5-21-2835300851-3378749978-4166134816

dn: ou=hosts,dc=smartbee,dc=com
objectClass: organizationalUnit
ou: hosts
description: Computer List
---------- end of smbldap.ldif ----------

[root@ldap ~]# rm -f /var/lib/ldap/*
[root@ldap ~]# ldapadd -x -D"cn=Manager,dc=smartbee,dc=com" -W -f smbldap.ldif
Enter LDAP Password:
adding new entry "dc=smartbee,dc=com"

adding new entry "ou=people,dc=smartbee,dc=com"

adding new entry "ou=Idmap,dc=smartbee,dc=com"

adding new entry "ou=groups,dc=smartbee,dc=com"

adding new entry "sambaDomainName=SMARTBEE,dc=smartbee,dc=com"

adding new entry "ou=hosts,dc=smartbee,dc=com"

[root@ldap ~]# smbldap-populate
Populating LDAP directory for domain SMARTBEE (S-1-5-21-2835300851-3378749978-4166134816)
(using builtin directory structure)

adding new entry: dc=smartbee,dc=com
adding new entry: ou=People,dc=smartbee,dc=com
adding new entry: ou=Group,dc=smartbee,dc=com
adding new entry: ou=Hosts,dc=smartbee,dc=com
adding new entry: ou=Idmap,dc=smartbee,dc=com
adding new entry: uid=root,ou=People,dc=smartbee,dc=com
adding new entry: uid=nobody,ou=People,dc=smartbee,dc=com
adding new entry: cn=Domain Admins,ou=Group,dc=smartbee,dc=com
adding new entry: cn=Domain Users,ou=Group,dc=smartbee,dc=com
adding new entry: cn=Domain Guests,ou=Group,dc=smartbee,dc=com
adding new entry: cn=Domain Computers,ou=Group,dc=smartbee,dc=com
adding new entry: cn=Administrators,ou=Group,dc=smartbee,dc=com
adding new entry: cn=Account Operators,ou=Group,dc=smartbee,dc=com

adding new entry: cn=Print Operators,ou=Group,dc=smartbee,dc=com
adding new entry: cn=Backup Operators,ou=Group,dc=smartbee,dc=com
adding new entry: cn=Replicators,ou=Group,dc=smartbee,dc=com
adding new entry: sambaDomainName=SMARTBEE,dc=smartbee,dc=com

Please provide a password for the domain root:
Changing UNIX and samba passwords for root
New password:
Retype new password:
[root@ldap ~]# /etc/init.d/ldap start

Selamat Backend LDAP Anda telah siap digunakan……

Uji Coba PDC Samba menggunakan Backend LDAP……

Kita akan mencoba PDC dengan menggunakan windows 98 sebagai client, langkah pertama membuat User untuk menguji coba seluruh konfigurasi Anda, bandingkan hasilnya dengan konfigurasi pada artikel *Pengenalan LDAP*.

[root@ldap ~]# smbldap-useradd -a rsukmana
[root@ldap ~]# smbldap-passwd rsukmana
Changing UNIX and samba passwords for rsukmana
New password:
Retype new password:

[root@ldap ~]# ldapsearch -x uid=rsukmana
extended LDIF
#
LDAPv3
base <> with scope sub
filter: uid=rsukmana
requesting: ALL
#

rsukmana, People, smartbee.com
dn: uid=rsukmana,ou=People,dc=smartbee,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: sambaSamAccount
cn: rsukmana

sn: rsukmana
givenName: rsukmana
uid: rsukmana
uidNumber: 1000
gidNumber: 513
homeDirectory: /home/rsukmana
loginShell: /bin/bash
gecos: Smartbee User
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
displayName: Smartbee User
sambaSID: S-1-5-21-2835300851-3378749978-4166134816-3000
sambaPrimaryGroupSID: S-1-5-21-2835300851-3378749978-4166134816-513
sambaProfilePath: \\LDAP\profiles\rsukmana
sambaHomePath: \\LDAP\rsukmana
sambaHomeDrive: P:
sambaLMPassword: 8F9EA0811C8C9E99AAD3B435B51404EE
sambaAcctFlags: [U]
sambaNTPassword: E8A37C0F5A88CCFEF78FD7DB51F16AB2
sambaPwdLastSet: 1168088821
sambaPwdMustChange: 1171976821
userPassword:: Ym9uam92aQ==

search result
search: 2
result: 0 Success

numResponses: 2
numEntries: 1
[root@ldap ~]# ldapsearch -x

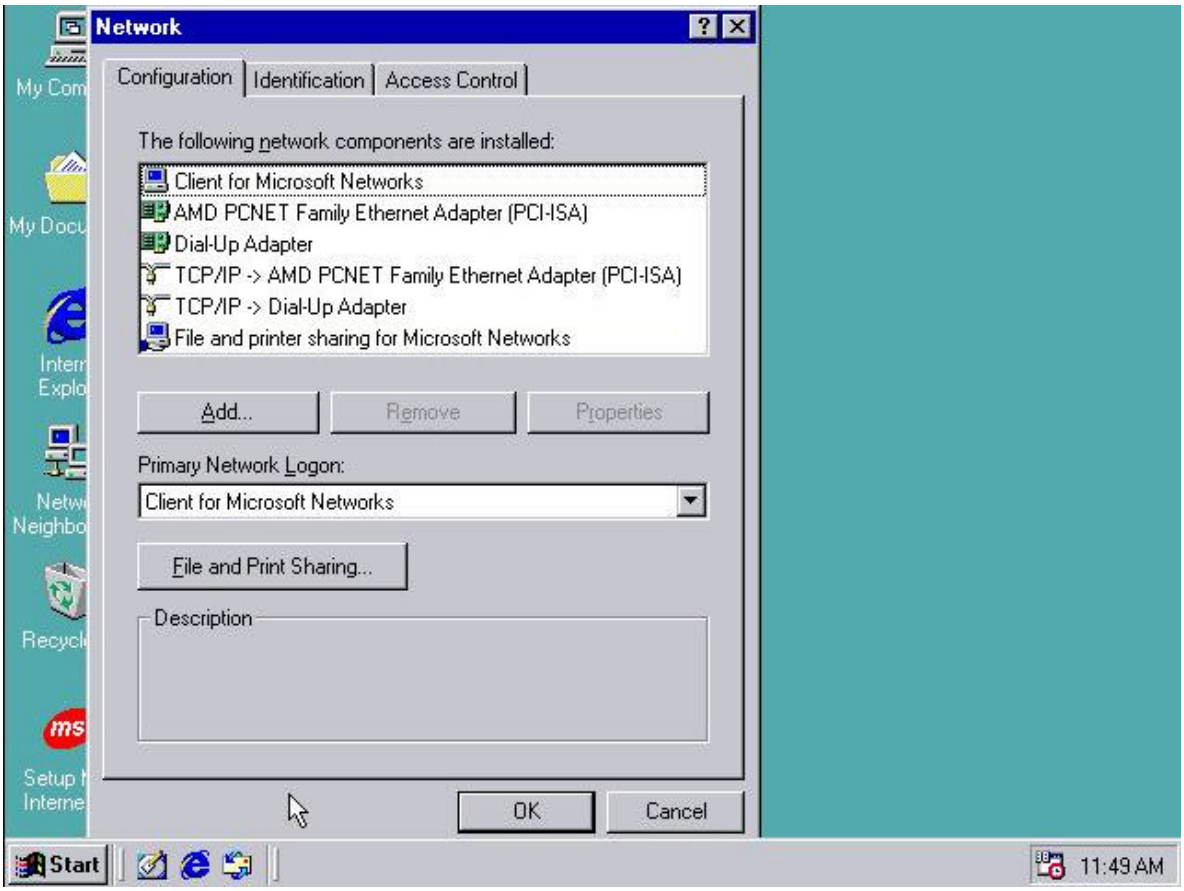
Silahkan Anda lanjutkan buat user berikutnya

Konfigurasi Windows Client untuk login ke domain……

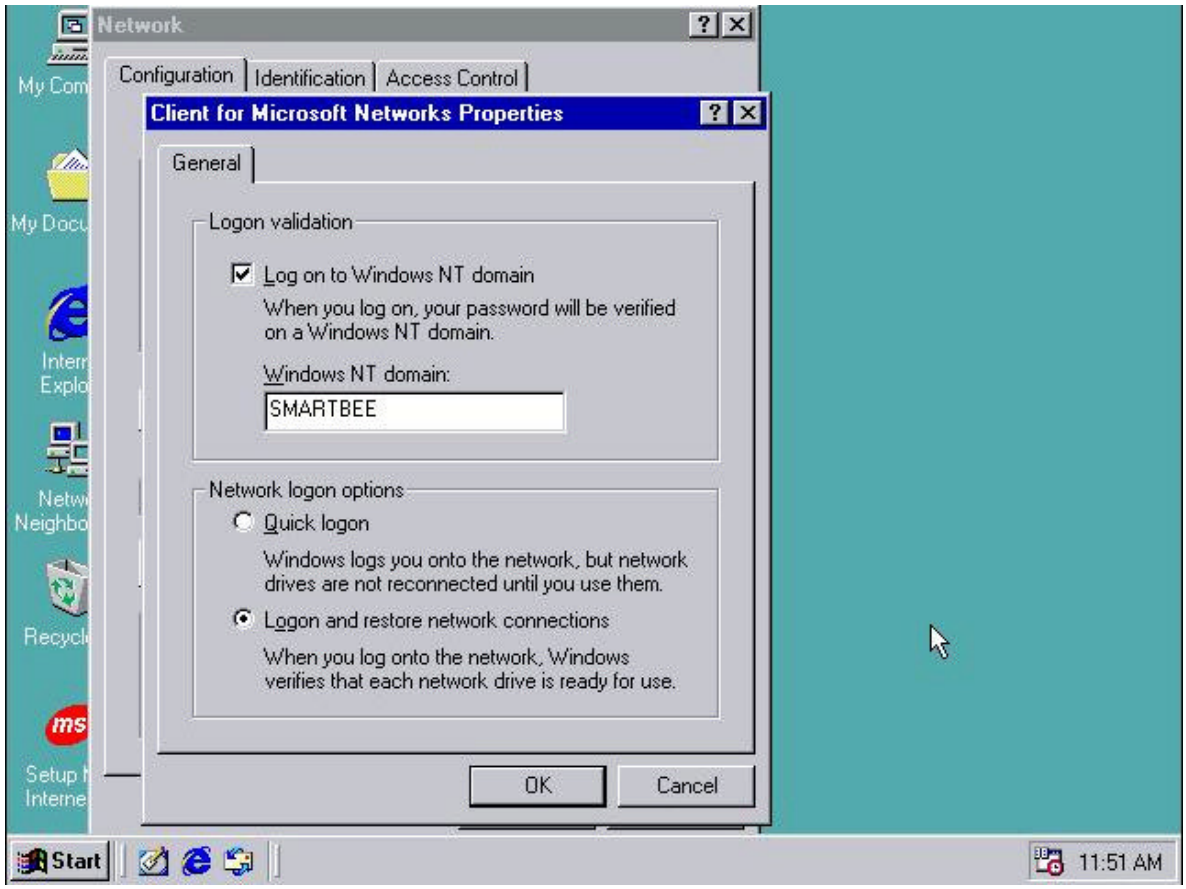
Kita akan coba konfigurasikan satu mesin Windows 98 agar dapat login menggunakan otentikasi user dari samba PDC yang telah Anda buat, contoh gambarnya dapat Anda lihat pada gambar 1 yang ada diatas.

Aktifkan Windows 98 Anda, dan pastikan network telah terkoneksi dengan baik, lalu lakukan konfigurasi sebagai berikut :

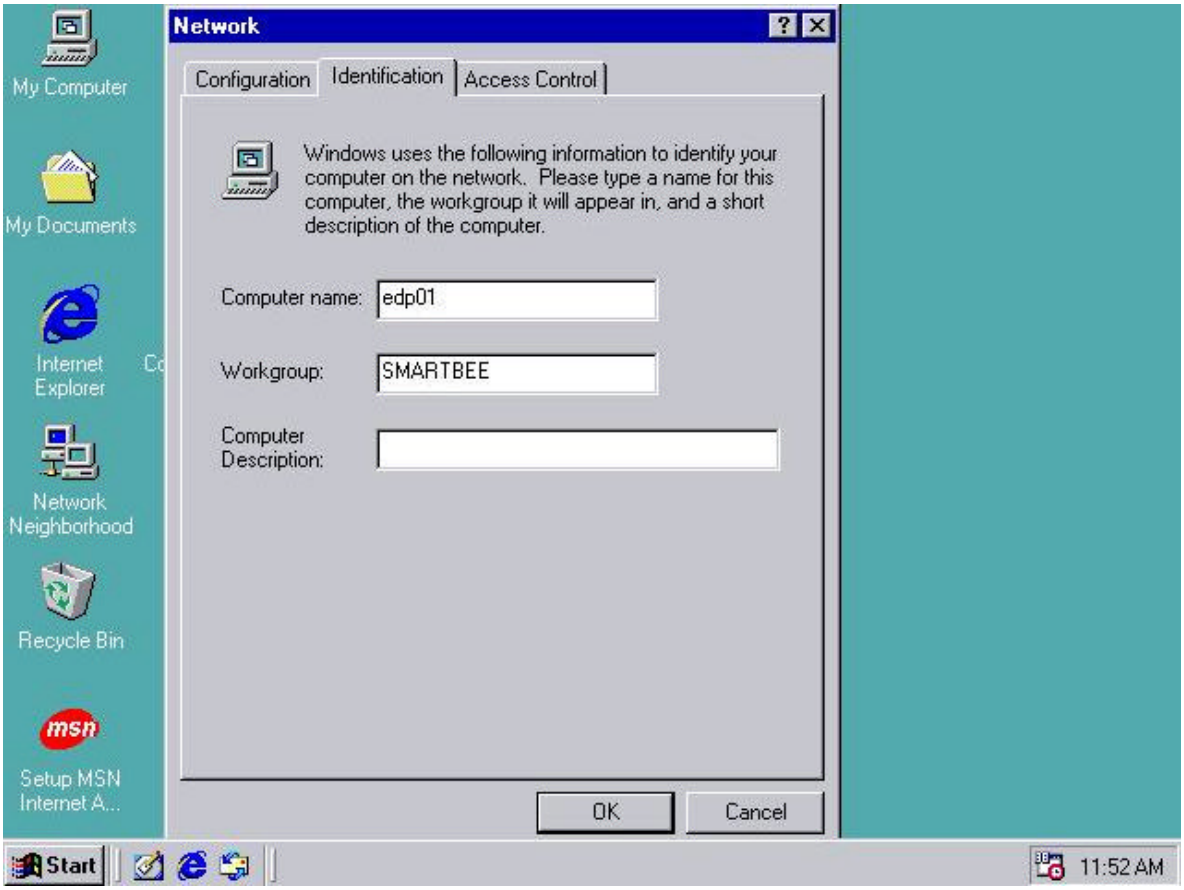
1. ***Start > Settings > Control Panel > Network***



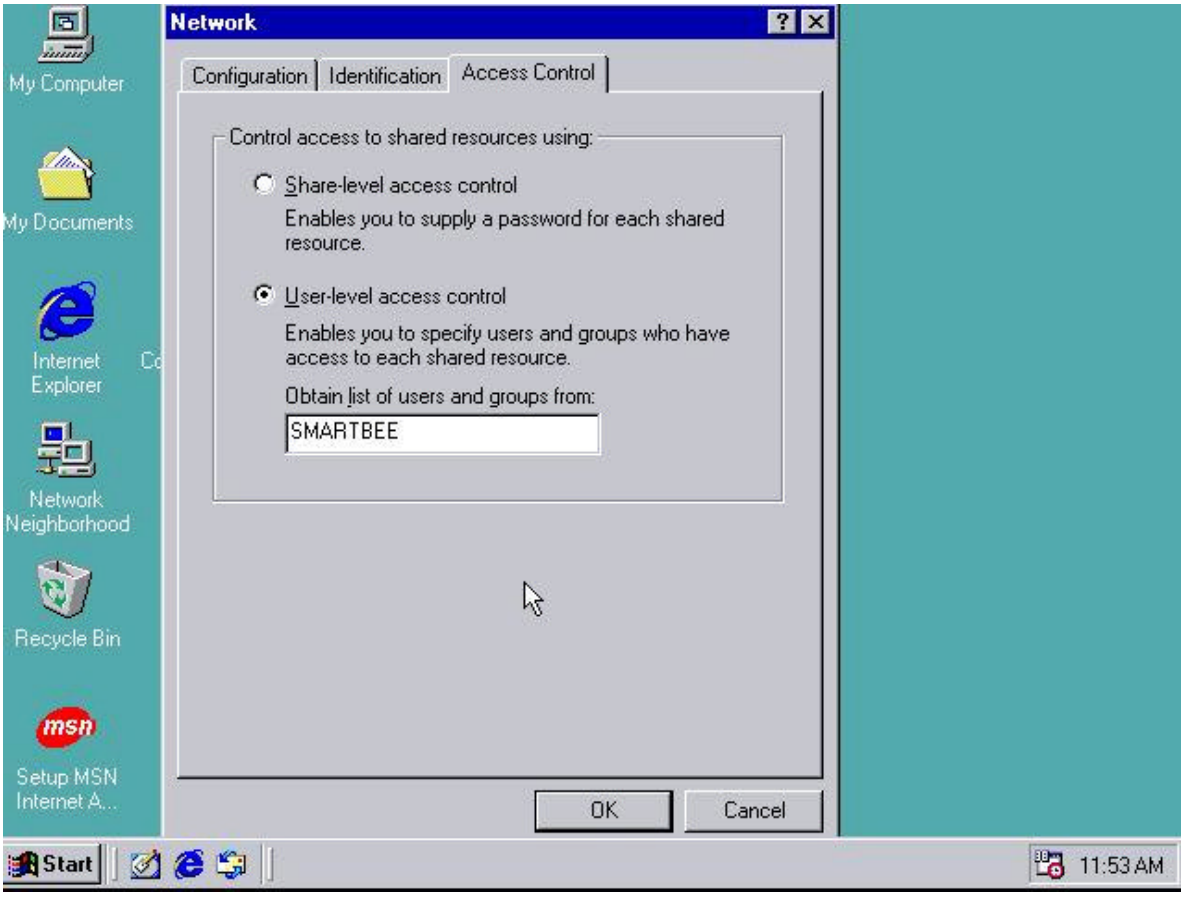
2. Pilih ***Client for Microsoft Network***, lalu check list ***Log on Windows NT Domain***, dan ketiklah SMARTBEE (nama domain Anda) pada baris ***Windows NT Domain***



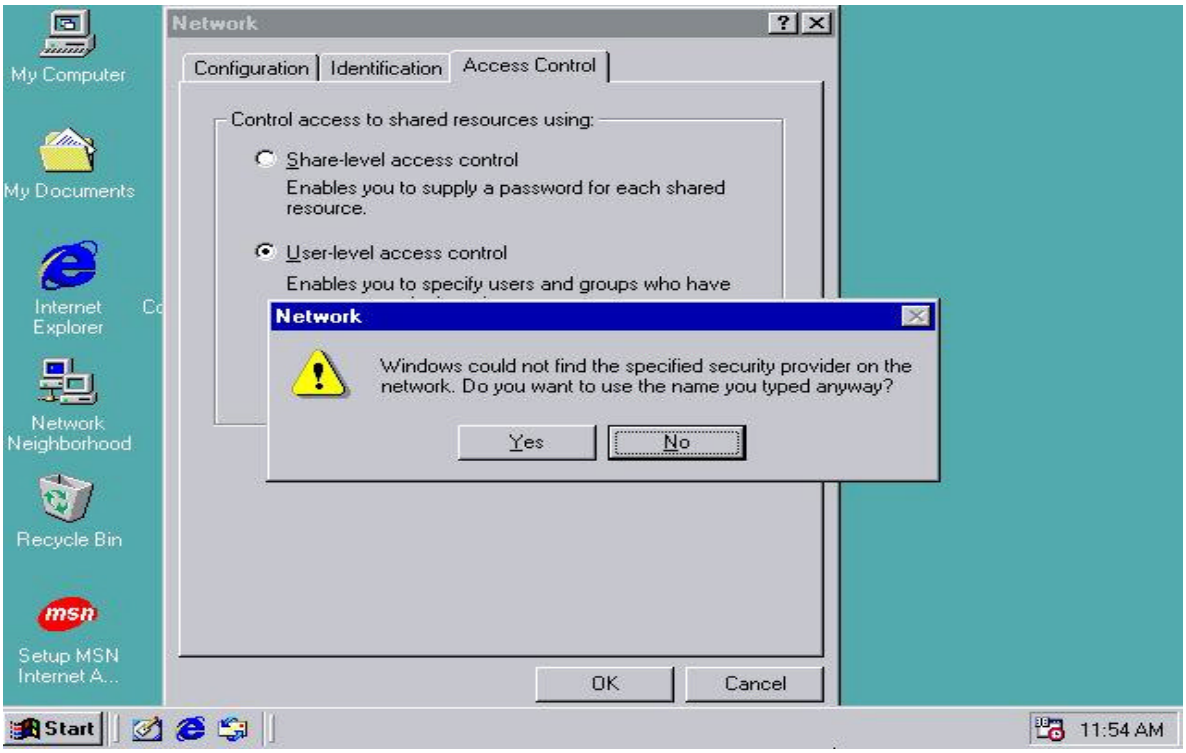
3. Sekarang Anda pindah ke tab ***Identification*** lalu silahkan Anda ketikkan edp01 pada Computer Name dan ketiklah SMARTBEE (Nama Group Komputer Anda). Setelah mempelajari teori yang telah di bahas sebelumnya, Penulis harap Anda akan memahami fungsi dari konfigurasi pada tab ***Identification*** ini.

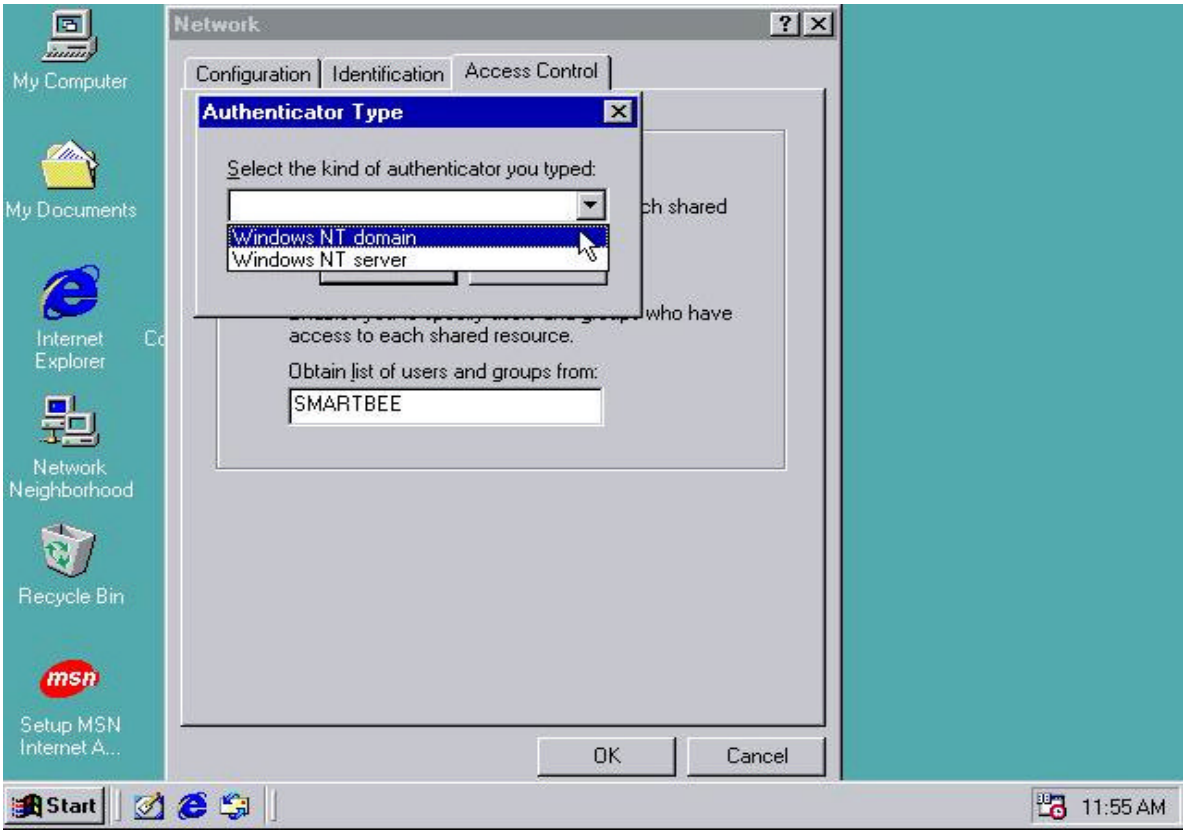


4. Sekarang Anda pindah ke tab ***Access Control*** lalu check list *User-level Acceess Contol* dan ketiklah SMARTBEE (Nama Domain Anda) pada *Obtain List of users and groups from*. Tahapan ini menunjukan ciri dari jaringan domain yaitu tingkat keamanannya tersentral, sehingga pungaaturan sekuritas dan sumber daya terpusat menggunakan autorisasi Domain.

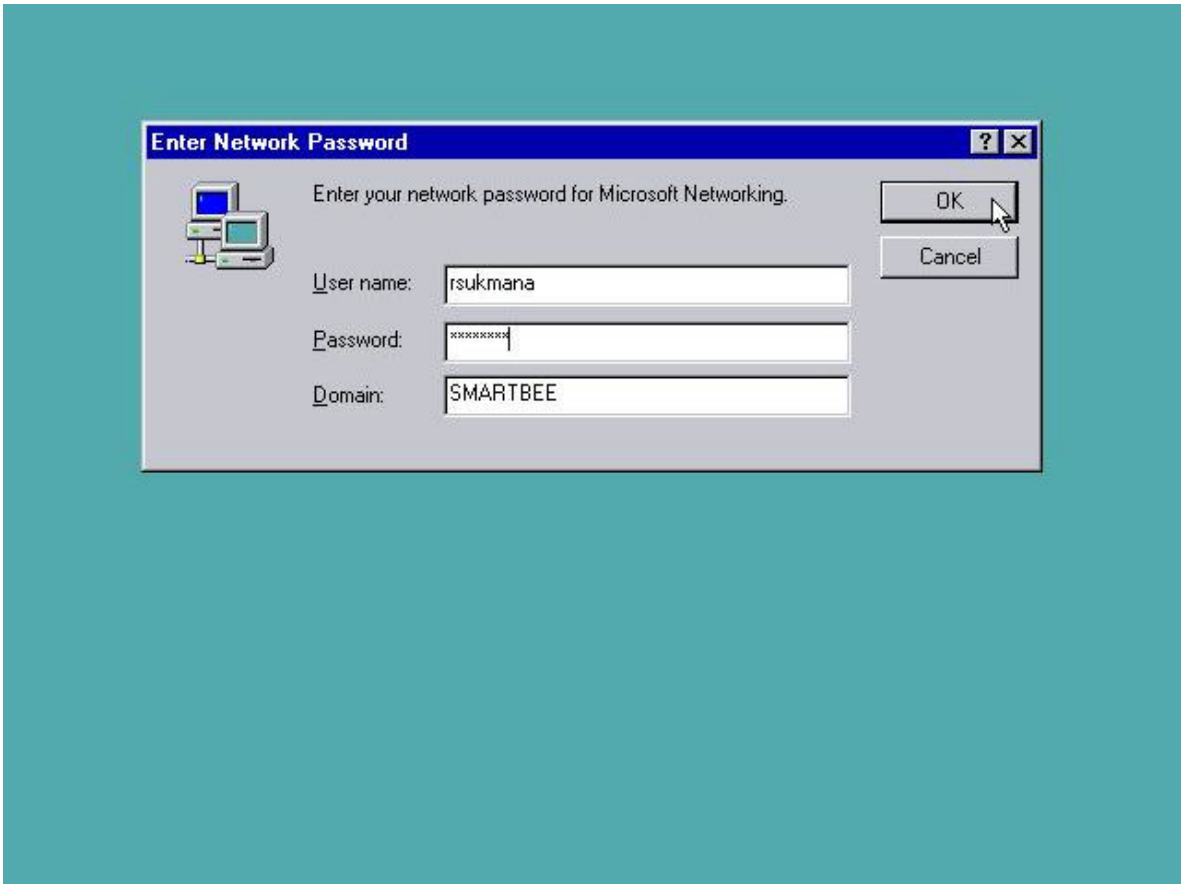


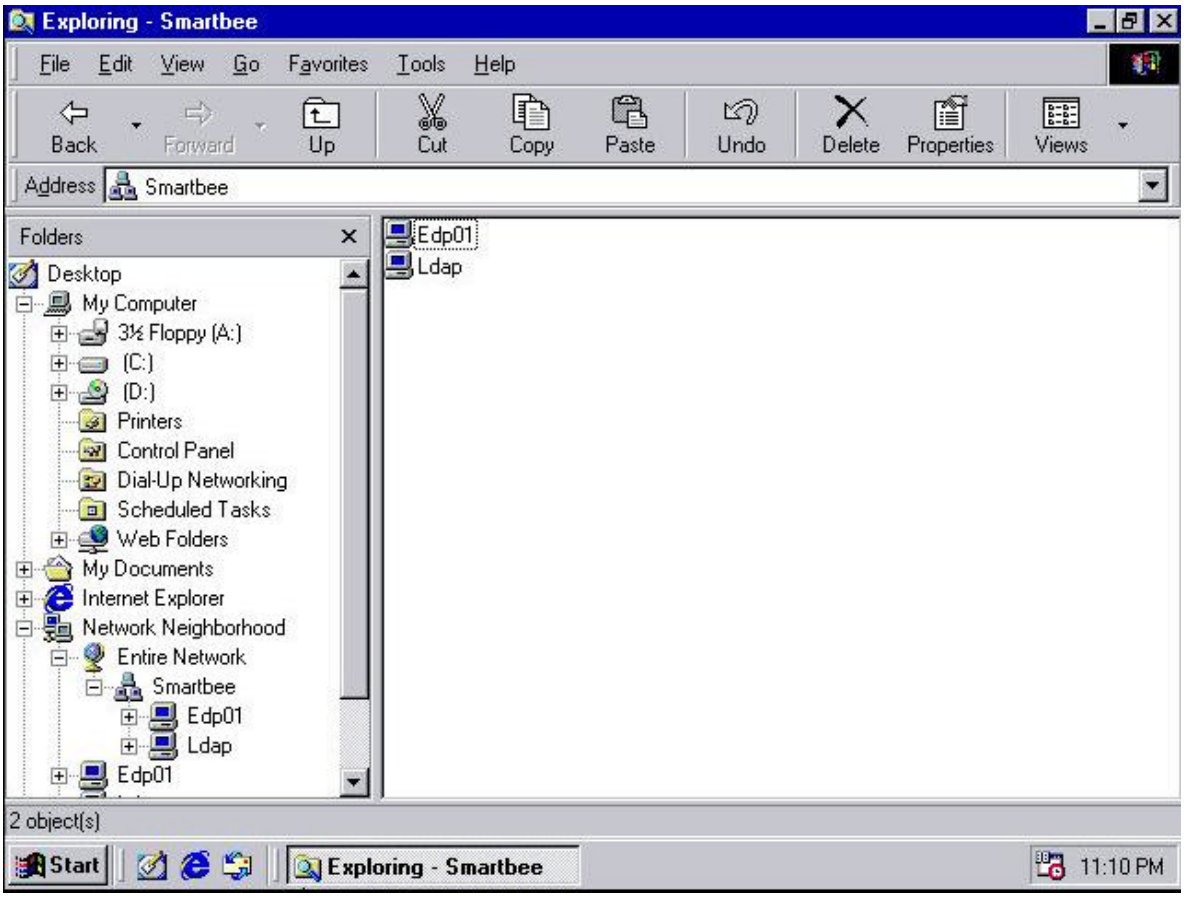
Setelah Anda tekan tombol *OK*, maka akan muncul peringatan yang menyatakan client Anda tidak dapat menemukan Domain yang menyediakan layanan autorisasi. Anda dapat menekan tombol *OK* dan pilih *Windows NT Domain*.





Setelah Anda tekan *OK* dan restart komputer Anda, maka Anda akan menjumpai form login yang di atur oleh Domain server. Login-lah menggunakan user yang telah Anda buat sebelumnya dan apabila berhasil, coba Anda buka Windows Explorer dan lihat isi dari *network neighborhood* Anda. Dari tampilan yang Anda lihat, penulis harap Anda sudah dapat mengetahui protokol apa saja yang bekerja sesuai dengan teori yang telah Anda pelajari sebelumnya.





Semoga membantu …….

06-01-2007:23.30

Referensi

- Eckstein, Robert. Collier-Brown, David. Kelly, Peter. *Using Samba*: O'Reilly
- Jackiewicz, Tom. *Deploying OpenLDAP*. United States: Apress, 2005
- Sharpe, Richard *Just what is SMB*
- Sofyan, Ahmad *Server Linux*

Biografi Penulis

Ratdhian Cipta Sukmana.
Mempelajari Ilmu Komputer berawal dari hobi, sejak SMU telah mengikuti pelatihan-pelatihan komputer hingga akhirnya dapat menyelesaikan S1 pada jurusan System Komputer Universitas Gunadarma Jakarta di akhir tahun 2001. Memulai karirnya sebagai Technical Support di beberapa perusahaan dan hingga kini masih aktif sebagai staff IT salah satu perusahaan Media di Jakarta. Sangat tertarik dengan Open Source dan Networking. Kopetensi inti pada bidang IT Support, Network Security, Administrator dan System Developer. Aktif di berbagai milis, dan selalu berusaha menggemakan konsep keterbukaan akan ilmu pengetahuan dengan semangat "Open Content". Berbagai artikel komputasi menarik lain yang di tuliskan berdasarkan pengalaman tersedia di situs blog *http://ratdix.wordpress.com*