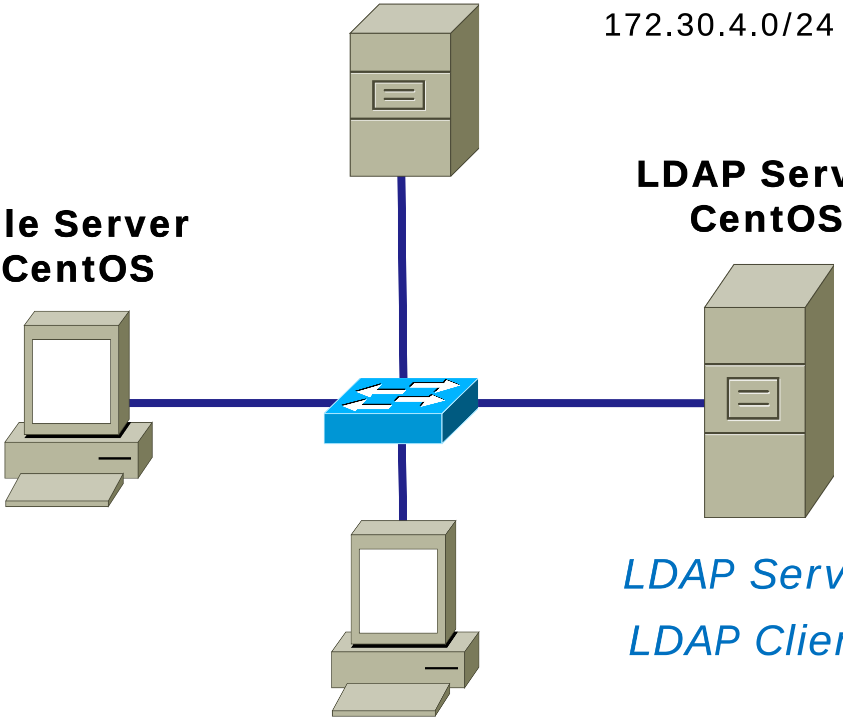
LDAP
(Lightweight Directory Access Protocol)

- LDAP is an Internet standard protocol used by applications to access information in a directory.
- It runs directly over TCP, and can be used to access a standalone LDAP directory service or to access a directory service.
- It was created as a way to minimize the implementation requirements on directory clients, and to simplify and encourage the use of directories services among applications.

LDAP

- Active Directory – Windows 2003 server
- LDAP – Server and Client
- LINUX Configuration File
- Samba
- Pam

LDAP
(Lightweight Directory Access Protocol)



Active Directory
Win Server 2003

172.30.4.0/24

File Server
CentOS

LDAP Server
CentOS

XP

LDAP Server

LDAP Client

LDAP - Server Installation

Install ldap

- rpm –hiv openldap-servers-2.3.43-3.e15.rpm
- rpm –hiv openldap-clients-2.3.43-3.e15.rpm

LDAP - Server Configuration

Edit the /etc/openldap/slap.conf file

```
database        bdb
directory       /var/lib/ldap
suffix          dc=acme,dc=com
rootdn          cn=Manager,dc=acme,dc=com
rootpw {SSHA}vv2y+i6V6esazrIv70xSSnNAJE18bb2u
```

LDAP - Server Configuration

Automatically start service at system boot

```
[root@acmeldap ~]# chkconfig --level 5 ldap on
```

LDAP – Server and Client Configuration

Changes to the /etc/pam_smb.conf file

This configuration consists of three lines the first containing the DOMAIN to be logged on at and the second and third are the primary and secondary servers to use. The server machines simply machines which can authenticate to the domain

<Domain>
<primary domain server>
< secondary domain server>

LDAP – Server and Client Configuration

Changes to the /etc/nsswitch.conf file

The change should be made only to the following three entries.

```
passwd: files ldap
shadow: files ldap
group: files ldap
```

When applications need information from /etc/passwd, /etc/shadow or /etc/groups, they will read the files directly then it will files and then look at LDAP

LDAP - Client Installation

Install the ldap

- rpm –hiv openldap-clients-2.3.43-3.e15.rpm

Install Samba and the dependencies

- rpm –hiv perl-Convert-ASNI-0.20-1.1.noarch.rpm
- rpm –hiv samba-3.0.33-3.14.e15.i386.rpm

LDAP - Client
Edit the LDAP Configuration File

/etc/ldap.conf file

- The directives that need to be edited or as follows for the client

```
uri ldap://<ip address of the LDAP server>
base dc=acme,dc=com
binddn cn=Manager,dc=acme,dc=com
bindpw <password>
```

LDAP - Client
Edit the Samba Configuration File

/etc/samba/smb.conf file

```
# workgroup = NT-Domain-Name or Workgroup-Name, eg: MIDEARTH
   workgroup = <Domain Name>
```

LDAP - Client
Edit the Pam Configuration File

The file that effects most configurations is the system-auth file in the /etc/pam.d directory. system_auth – the following is the configuration of this file

```
auth       required     pam_env.so
auth       sufficient   pam_unix.so nullok try_first_pass
auth       requisite    pam_succeed_if.so uid >= 500 quiet
auth       sufficient   pam_smb_auth.so use_first_pass nolocal
auth       required     pam_deny.so
account    required     pam_unix.so
account    sufficient   pam_localuser.so
account    sufficient   pam_succeed_if.so uid < 500 quiet
account    required     pam_permit.so

password   requisite    pam_cracklib.so try_first_pass retry=3
password   sufficient   pam_unix.so md5 shadow nullok try_first_pass use_authtok
password   required     pam_deny.so
session    optional     pam_keyinit.so revoke
session    required     pam_limits.so
session    [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session    required     pam_unix.so
```

LDAP - Client
Samba Service Configuration

Automatically start service at system boot

- [root@acmeldap ~]# **chkconfig --level 5 smb on**

LDAP - Database
Server Configuration

The LDAP comes with a utility called ldapadd that will create entries into the LDAP database, used to add entries while the LDAP server is running.

LDAP - Database
Server Configuration

Step one is to insert the domain objects and the People object into the database. Create a domain file in /etc/openldap/acme.ldif

```
dn: dc=cis160,dc=com
dc: cis160
description: LDAP Admin
objectClass: dcObject
objectClass: organizationalUnit
ou: rootobject
```

Create a People file to /etc/openldap/people.ldif

```
dn: ou=People, dc=acme,dc=com
ou: Peopledescription: Users of acme
objectClass: organizationalUnit
```

Once the file is configure then it can be loaded into database as follows.

```
ldapadd -x -D "cn=Manager,dc=acme,dc=com" -W -f  /etc/openldap/research.ldif
```

LDAP - Database
Server Configuration

The second step is to create a Manager of LDAP Sever in the database. The Manager name is the cn=Manager in the /etc/openldap/slapd.conf file rootdn cn=Manager,dc=acme,dc=com.

Create the file to load the information into the LDAP database. The file contents looks like the following:

```
dn: uid=Manager,ou=People,dc=acme,dc=com
uid: Manager
objectClass: account
```

Add the manager to the LDAP database as follows

```
ldapadd -x -D "cn=Manager,dc=acme,dc=com" –W - f /etc/openldap/manager.ldif
```

LDAP - Database
Server Configuration

The third step is to creating a LINUX user and password for the user

- useradd tchildex –d <home dir>
- passwd tchildex

These two command will create an entry in the passwd, shadow, and the group file in /etc

The fourth step is creating as user file for the user

- This is done by grep tchildex /etc/passwd > /etc/openldap/passwd.tchildex

Then convert the passwd.file to ldif (LDAP Data Interchange Format) file by using the Perl script that comes with the Centos distro.

/usr/share/openldap/migration/migrate_passwd.pl /etc/openldap/passwd.tchildex etc/openldap/tchildex.ldif

LDAP - Database
Server Configuration

The fifth step **Inserting Users Groups**

- Creating group user file to be loaded into the LDAP database
- grep tchildex /etc/group > /etc/openldap/group.tchildex

```
/usr/share/openldap/migration/migrate_group.pl /etc/openldap/group.tchildex
/etc/openldap/tchildexgrp.ldif.
```

Then load the file into the LDAP database

```
ldapadd -x -D "cn=Manager,dc=acme,dc=com" -W -f  /etc/openldap/tchildexgrp.ldif
```

LDAP – Database Testing
Server Configuration

Using getent

- getent passwd
- getent group

Using the search utility that comes with the LDAP Client to search for users In the LDAP database

- ldapsearch –x –h cisldap2 –b “dc=cis160,dc=com” “cn=tchildex”

LDAP
(Lightweight Directory Access Protocol)

Is it installed?

```
[root@cisldap2 ~]# rpm -qa | grep ldap
openldap-servers-2.3.43-3.e15.rpm
openldap-clients-2.3.43-3.e15.rpm
```

Is it running?

```
[root@cisldap2 ~]# ps -ef | grep ldap
root      5587      1  0 15:50 ?        00:00:00 /usr/sbin/ldapd
root      9911   5505  0 18:18 pts/0    00:00:00 grep ldap
```

```
[root@cisldap2 ~]# service ldap status
ldapd (pid 1636) is running...
```

LDAP
(Lightweight Directory Access Protocol)

Is it installed?

```
[root@cisldap2 ~]# rpm -qa | grep samba
rpm –hiv samba-3.0.33-3.14.e15.i386.rpm
```

Is it running?

```
[root@cisldap2 ~]# ps -ef | grep smb
root      5587      1  0 15:50 ?        00:00:00 smbd -D
root      9911   5505  0 18:18 pts/0    00:00:00 grep smb
```

```
[root@cisldap2 ~]# service smb status
smbd (pid 1858) is running...
```