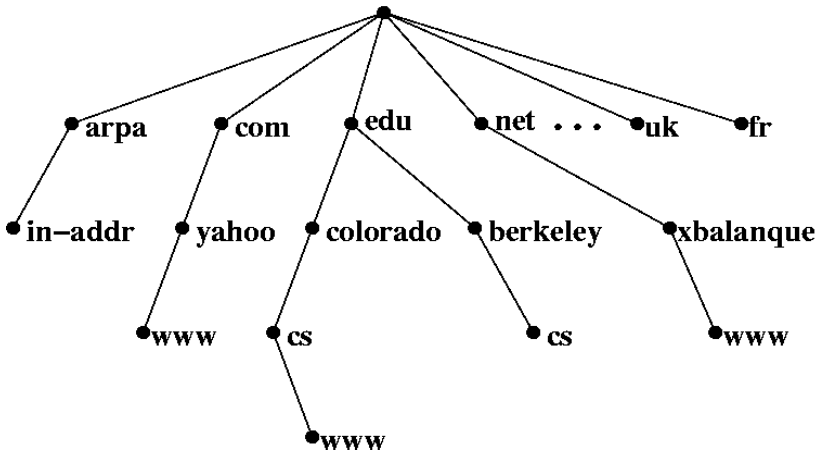
LDAP
(Lightweight Directory Access Protocol)

zjlin

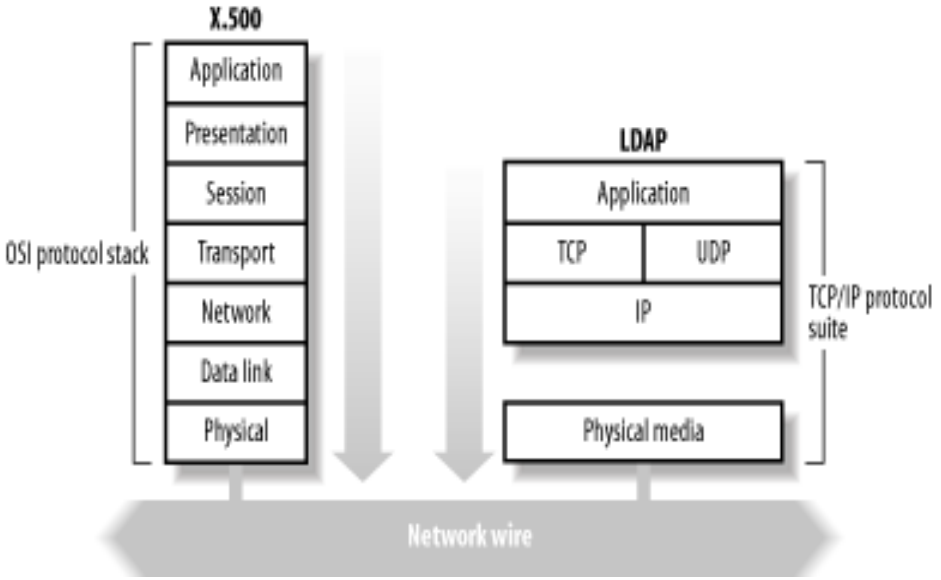
What is Directory Service?

- What is Directory Service (名錄服務)
  - A directory service is highly optimized for reads.
  - A directory service implements a distributed model for storing information.
  - A directory service has advanced search capabilities.
  - A directory service has loosely consistent replication among directory servers.
- Domain Name Service

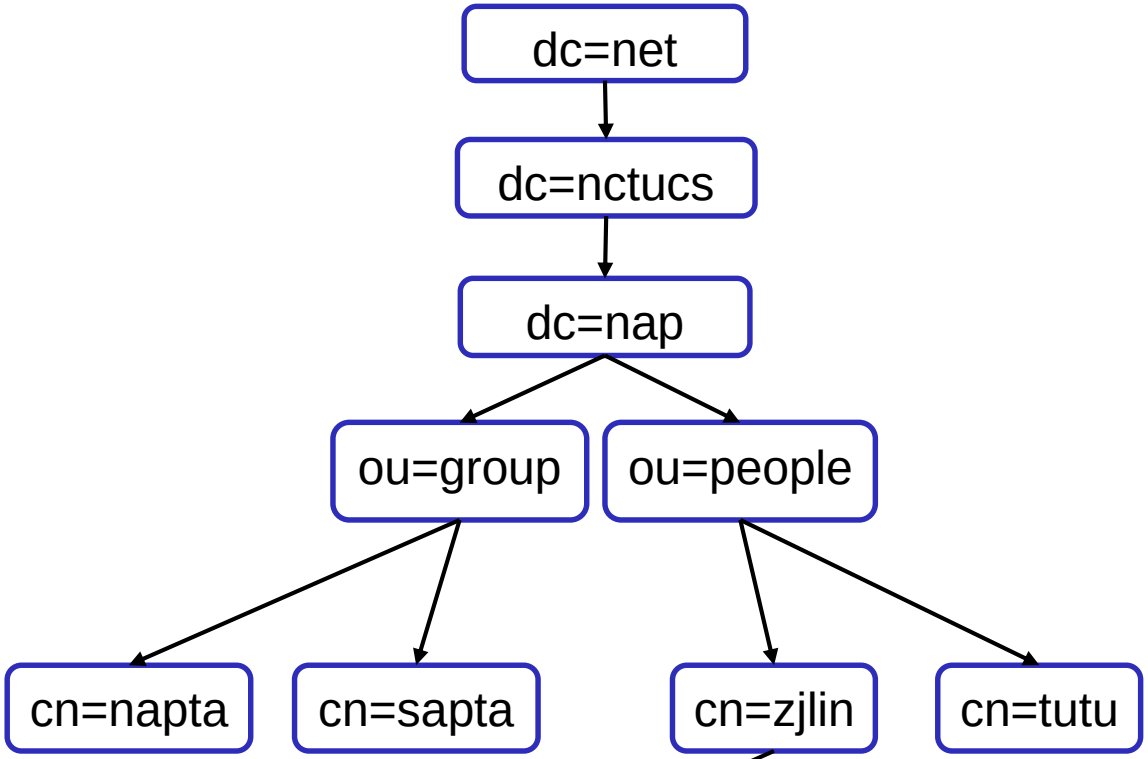


What is LDAP

- Lightweight Directory Access Protocol (LDAP)
  - LDAP v3: RFC 3377
  - RFC 2251-2256, 2829, 2830, 3377
- Why LDAP is lightweight
  - subset of X.500
  - X.500 base on OSI stack
  - LDAP base on TCP/IP
  - LDAP omits many X.500 operations that are rarely used
  - Providing a smaller and simpler set of operations

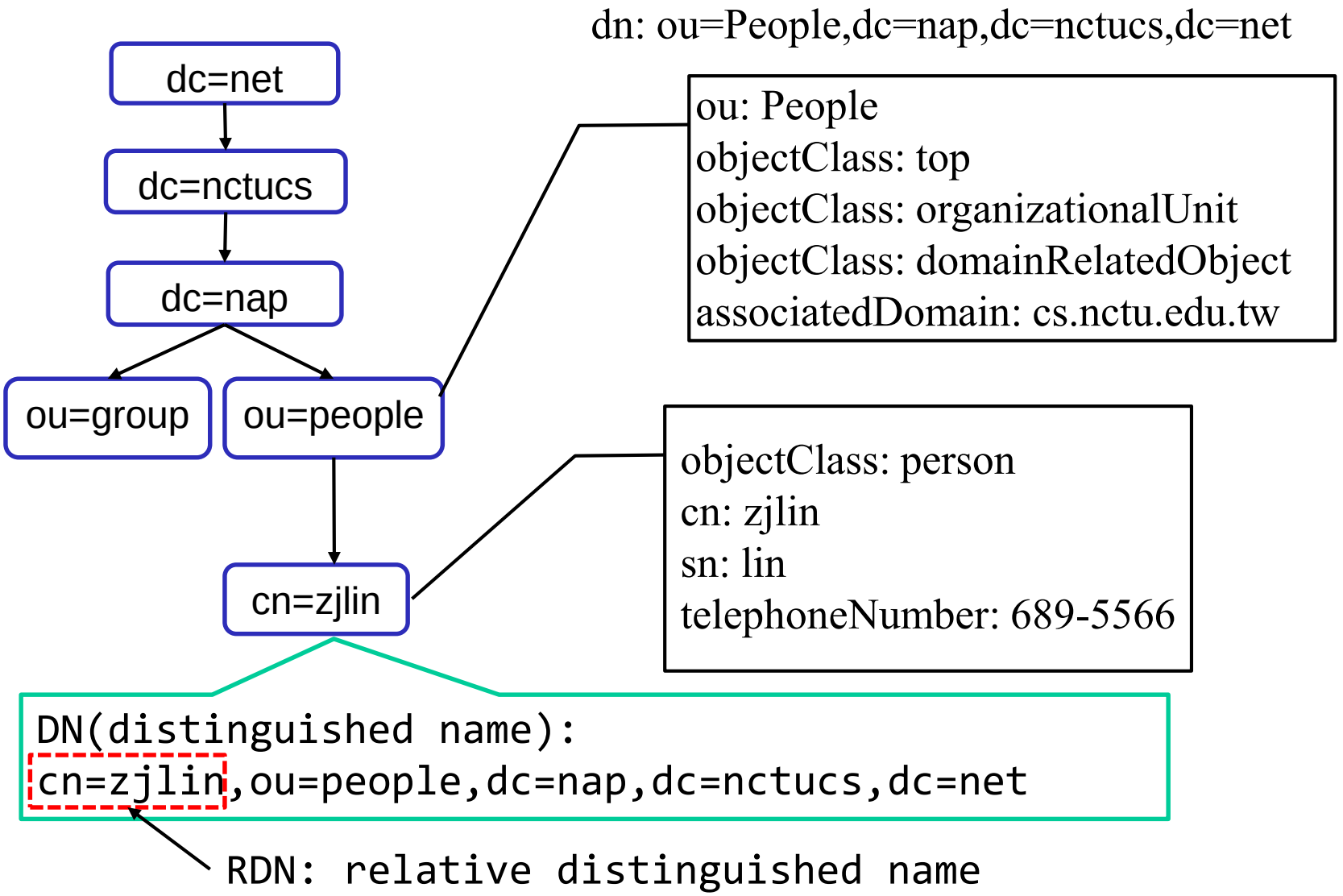


LDAP Directory Information Tree (DIT)




```
cn=zjlin,ou=people,dc=sap,dc=nctucs,dc=net
o="sap, nctucs, net", c=Taiwan
o=sap.nctucs.net
```

LDAP Directory Information Tree (DIT)



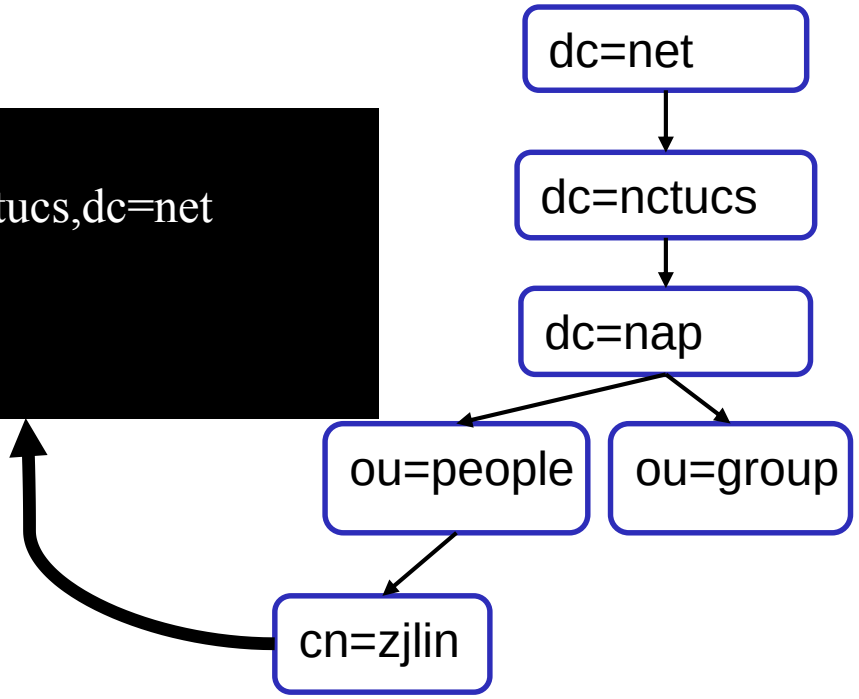
LDAPv3 overview – LDIF

- LDAP Interchange Format (LDIF)
  - Defined in RFC 2849
  - standard text file format for storing LDAP configuration information and directory contents
  - An LDIF file is
    1. A collection of entries separated from each other by blank lines
    2. A mapping of attribute names to values
    3. A collection of directives that instruct the parser how to process the information
  - The data in the LDIF file must obey the schema rules of your LDAP directory

LDAPv3 overview – LDIF

- Sample LDIF

```
# sample entry
dn: cn=zjlin,ou=people,dc=nap,dc=nctucs,dc=net
objectClass: person
cn: zjlin
telephoneNumber: 689-5566
```



dn: distinguished name
rdn: relative dn
ou: organizational unit
dc: domain component
cn: comman name

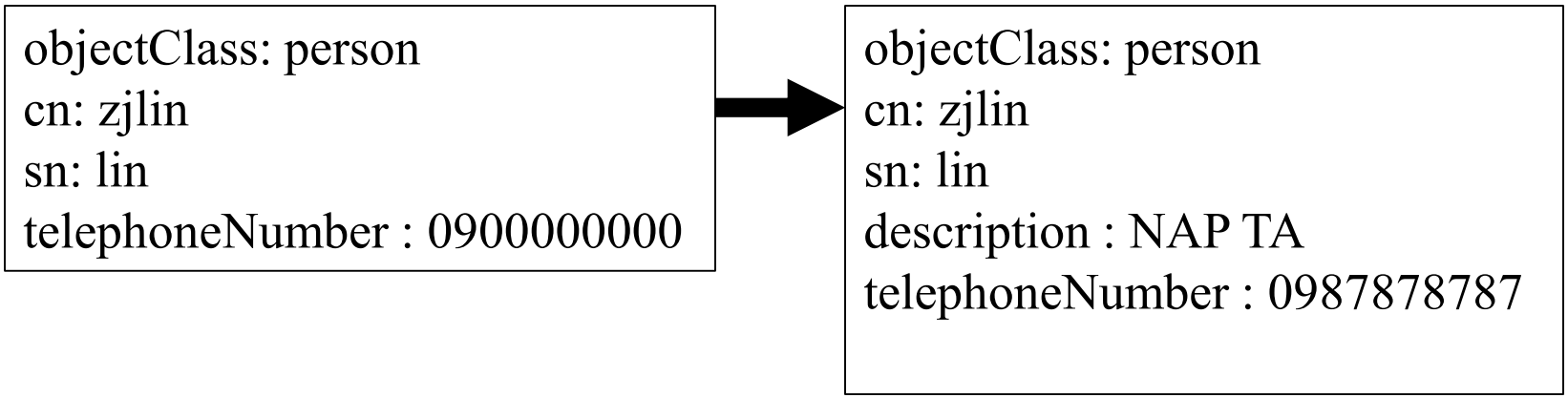
```
DN(distinguished name):
cn=zjlin,ou=people,dc=nap,dc=nctucs,dc=net
```

RDN: relative distinguished name

LDAPv3 overview – LDIF

- Sample LDIF - Modify one dn

```
# modify user info
dn: cn=zjlin,ou=people,dc=nap,dc=nctucs,dc=net
changetype: modify
add: description
description : NAP TA
-
replace: telephoneNumber
telephoneNumber : 0987878787
```



LDAPv3 overview – LDIF

- Sample LDIF - Modify more than one dn

```
# modify user info
dn: cn=zjlin,ou=people,dc=nap,dc=nctucs,dc=net
changetype: modify
add: description
description : NAP TA

dn: cn=tutu,ou=people,dc=nap,dc=nctucs,dc=net
changetype: modify
add: description
description : NAP TA
```

LDAPv3 overview - objectClass

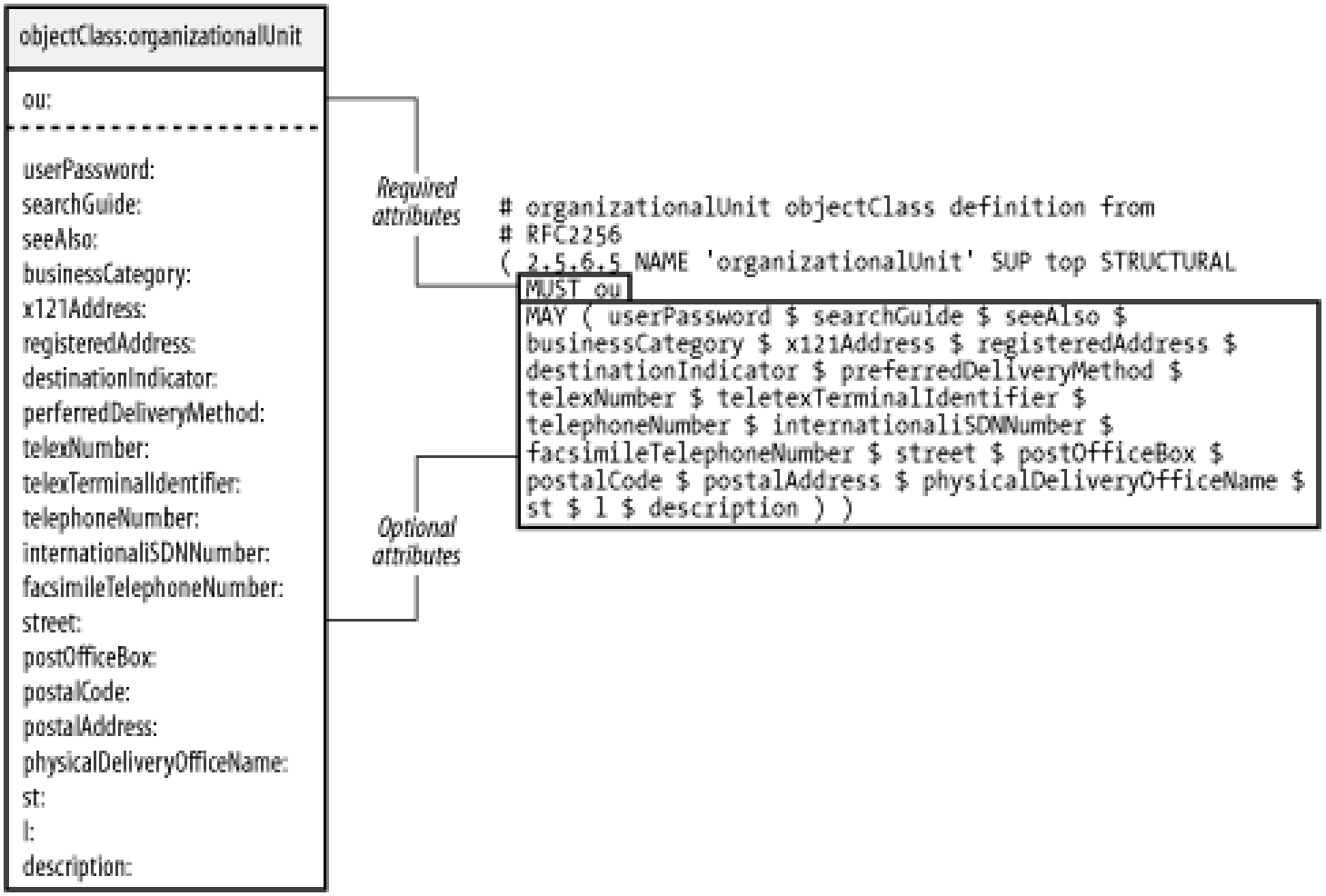
- /usr/local/etc/openldap/schema/core.schema

```
objectclass ( 2.5.6.6 NAME 'person'
        DESC 'RFC2256: a person'
        SUP top STRUCTURAL
        MUST ( sn $ cn )
        MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
```

```
ObjectClassDescription = "(" whsp
        numericoid whsp      ; ObjectClass identifier
        [ "NAME" qdescrs ]
        [ "DESC" qdstring ]
        [ "OBSOLETE" whsp ]
        [ "SUP" oids ]       ; Superior ObjectClasses
        [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ]
                ; default structural
        [ "MUST" oids ]      ; AttributeTypes
        [ "MAY" oids ]       ; AttributeTypes
        whsp ")"
```

http://www.openldap.org/doc/admin24/schema.html

LDAPv3 overview - objectClass



http://www.openldap.org/doc/admin24/schema.html

LDAPv3 overview - Attribute

```
attributetype ( 2.5.4.20 NAME 'telephoneNumber'
        DESC 'RFC2256: Telephone Number'
        EQUALITY telephoneNumberMatch
        SUBSTR telephoneNumberSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.50{32} )
```

Matching rules

Type

Server should support values of this length

Table 8.3: Commonly Used Syntaxes

Name	OID	Description
boolean	1.3.6.1.4.1.1466.115.121.1.7	boolean value
directoryString	1.3.6.1.4.1.1466.115.121.1.15	Unicode (UTF-8) string
distinguishedName	1.3.6.1.4.1.1466.115.121.1.12	LDAP DN
integer	1.3.6.1.4.1.1466.115.121.1.27	integer
numericString	1.3.6.1.4.1.1466.115.121.1.36	numeric string
OID	1.3.6.1.4.1.1466.115.121.1.38	object identifier
octetString	1.3.6.1.4.1.1466.115.121.1.40	arbitary octets

http://www.openldap.org/doc/admin24/schema.html

Comparison with relational databases

- It is tempting to think that having a RDBMS backend to the directory solves all problems. However, it is wrong.
- This is because the data models are very different. Representing directory data with a relational database is going to require splitting data into multiple tables.

OpenLDAP

- Installation
  - pkg install openldap-server
  - cd /usr/ports/net/openldap-server24 ; make install clean
- slap.conf
  - Blank lines and lines beginning with a pound sign (#) are ignored
  - Parameters and associated values are separated by whitespace characters
  - A line with a blank space in the first column is considered to be a continuation of the previous one.

slap.conf

```
include         /usr/local/etc/openldap/schema/core.schema
pidfile         /var/run/openldap/slapd.pid
argsfile        /var/run/openldap/slapd.args
loglevel        256
modulepath      /usr/local/libexec/openldap
moduleload      back_mdb
moduleload      back_ldap
# ACL rules here for global
database        mdb
maxsize         1073741824
suffix          "dc=nap,dc=nctucs,dc=net“
rootdn          "cn=Manager,dc=nap,dc=nctucs,dc=net"
roopw           <generated by slappasswd>
directory       /var/db/openldap-data

# Indices to maintain
index           objectClass eq
# ACL rules here for specify database
```

Directory ACL

```
access to dn.exact="cn=Manager,dc=nap,dc=nctucs,dc=net"
        by peername.ip=“127.0.0.1" auth
        by users none
        by anonymous none
        by * none

access to attrs=userPassword
        by self write
        by anonymous auth
        by dn.base="cn=Manager,dc=nap,dc=nctucs,dc=net" write
        by * none

access to attrs=englishname,birthdate
        by self write
        by users read
        by anonymous read
```

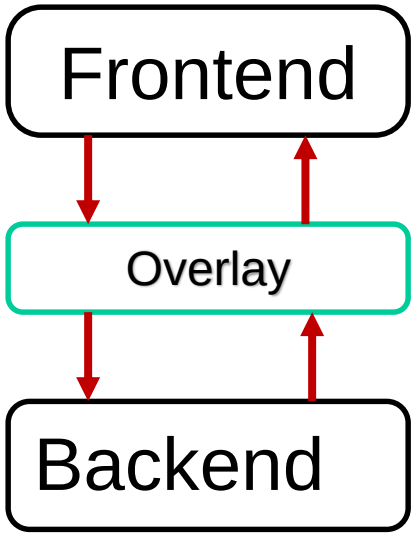
Directory ACL

Level	Privileges	Description
none =	0	no access
disclose =	d	needed for information disclosure on error
auth =	dx	needed to authenticate (bind)
compare =	cdx	needed to compare
search =	scdx	needed to apply search filters
read =	rscdx	needed to read search results
write =	wrscdx	needed to modify/rename
manage =	mwrscdx	needed to manage

http://www.openldap.org/doc/admin24/access-control.html

Overlay

- Software components that provide hooks to functions analogous to those provided by backends, which can be stacked on top of the backend calls and as callbacks on top of backend responses to alter their behavior.
- Frontend
  - handles network access and protocol processing
- Backend
  - deals strictly with data storage

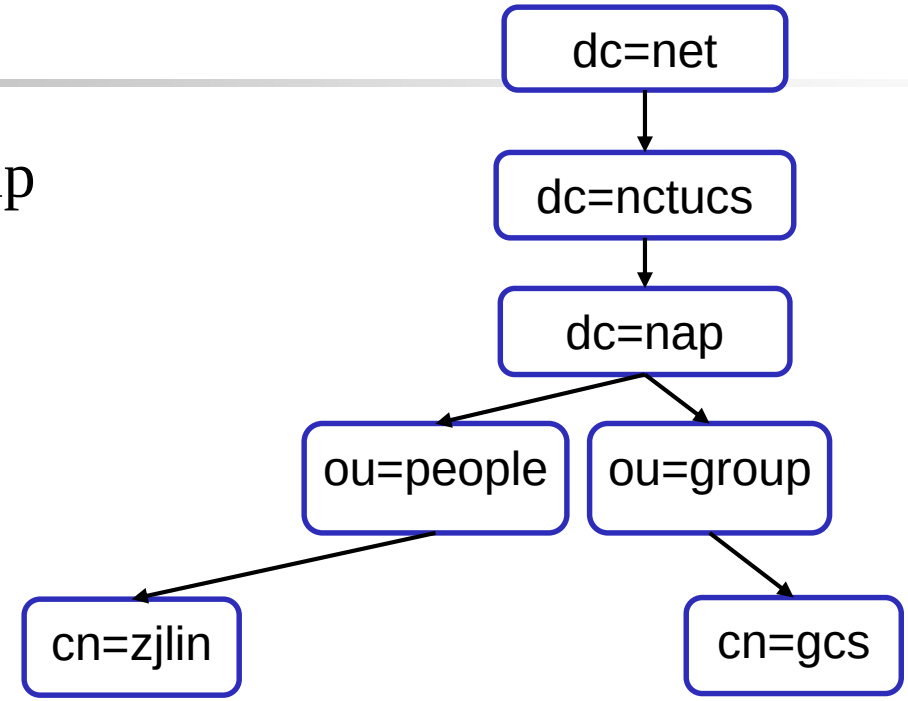


https://www.openldap.org/doc/admin24/overlays.html

https://en.wikipedia.org/wiki/OpenLDAP#Overlays

Overlay - memberOf

- Membership



objectClass: posixGroup
objectClass: top
objectClass: posixAccount
cn: zjlin
gidNumber: 1120

objectClass: posixGroup
objectClass: top
cn: gcs
displayName: gcs
description: Domain Unix group
gidNumber: 1120

Overlay - memberOf

- Installation
  - Ports
  - make config -> enable option

```
+[ ] LMPASSWD          With LM hash password support (DEPRECATED)
+[x] MDB               With Memory-Mapped DB backend
+[ ] MEMBEROF          With Reverse Group Membership overlay
+[ ] ODBC              With SQL backend
+[ ] OUTLOOK           Force caseIgnoreOrderingMatch on name attribute
+[ ] PASSWD            With Passwd backend
+[ ] PERL              With Perl backend
+[ ] PPOLICY           With Password Policy overlay
+[ ] PROXYCACHE        With Proxy Cache overlay
+[ ] REFINT            With Referential Integrity overlay
+[ ] RELAY             With Relay backend
+[ ] RETCODE           With Return Code testing overlay
```

https://www.openldap.org/doc/admin24/overlays.html

Overlay - memberOf

- slapd.conf

```
166 # MemberOf
167 overlay memberof
```

- restart slapd
- Schema

```
dn: cn=testgroup,ou=MemberGroup,dc=nap,dc=nctucs,dc=net
objectclass: groupOfNames
cn: testgroup
member: cn=zjlin,ou=People,dc=nap,dc=nctucs,dc=net
```

https://www.openldap.org/doc/admin24/overlays.html

OLC - on-line configuration

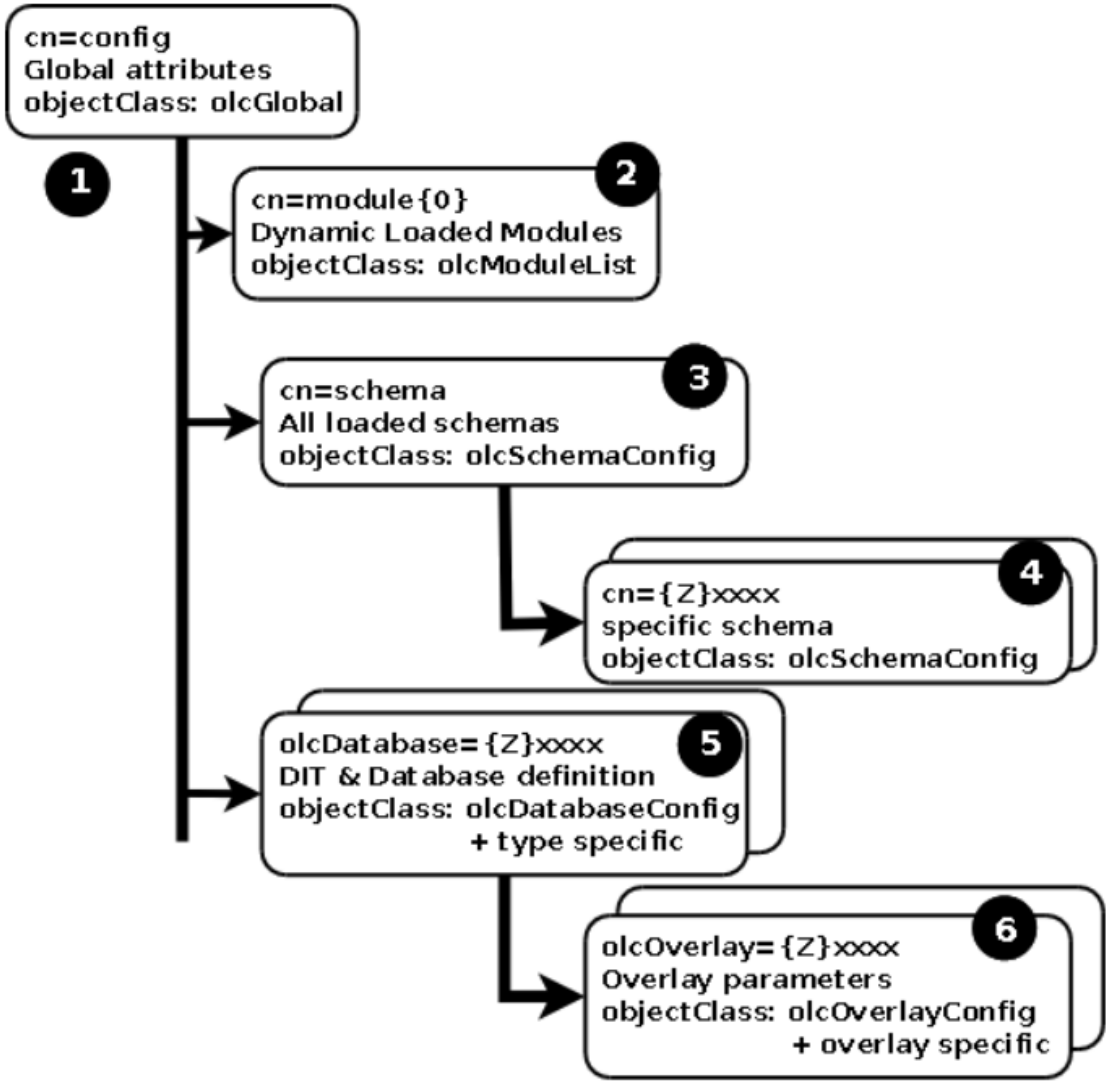
- OpenLDAP version 2.3 -> new feature
- OpenLDAP version 2.4 -> still optional

- Uses a configuration DIT to control the operational configuration
- Modifying entries in this DIT immediate changes to slapd's operational

https://www.openldap.org/doc/admin24/slapdconf2.html

http://www.zytrax.com/books/ldap/ch6/slapd-config.html

OLC - on-line configuration



OLC - on-line configuration

```
# {1}mdb, config
dn: olcDatabase={1}mdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcMdbConfig
olcDatabase: {1}mdb
olcDbDirectory: /var/db/openldap-data/cs
olcSuffix: dc=cs,dc=nctu,dc=edu,dc=tw
olcAddContentAcl: FALSE
olcLastMod: TRUE
olcMaxDerefDepth: 15
olcReadOnly: FALSE
olcRootDN: cn=Manager,dc=nap,dc=nctucs,dc=net
olcRootPW: password
```

Enable slapd

- Edit /etc/rc.conf
  - slapd_enable="YES"
  - slapd_flags for specific options
- service slapd start

http://www.openldap.org/doc/admin24/runningslapd.html

Slapd tools

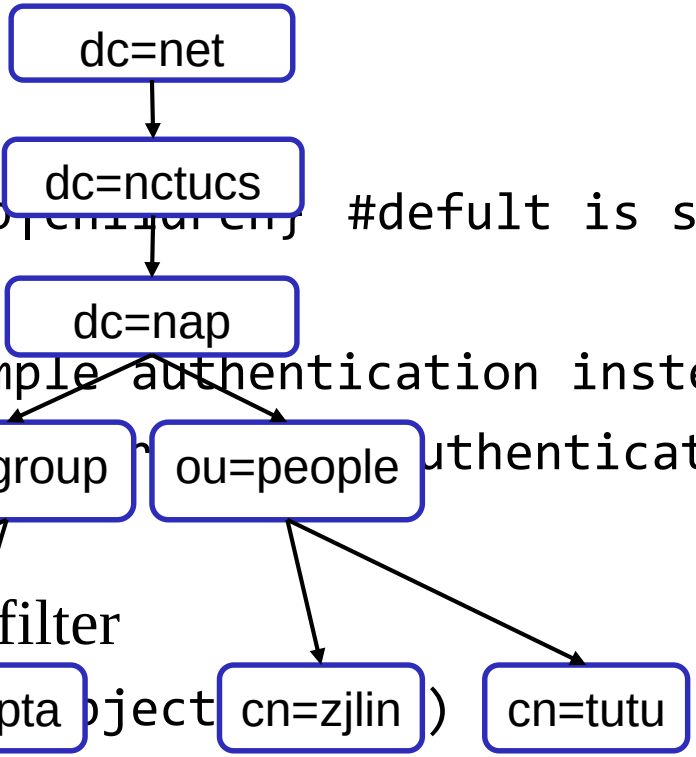
- slapcat
  - This tool reads records from a slapd database and writes them to a file or standard output
- slapadd
  - This tool reads LDIF entries from a file or standard input and writes the new records to a slapd database
- slapindex
  - This tool regenerates the indexes In a slapd database
- slappasswd
  - This tool generates a password hash suitable for use as an Lq in slapd.conf

LDAP tools

- ldapsearch
  - This tool issues LDAP search queries to directory servers
- ldapadd, ldapmodify
  - These tools send updates to directory servers
- ldapcompare
  - This tool asks a directory server to compare two values
- ldapdelete
  - This tool deletes entries from an LDAP directory

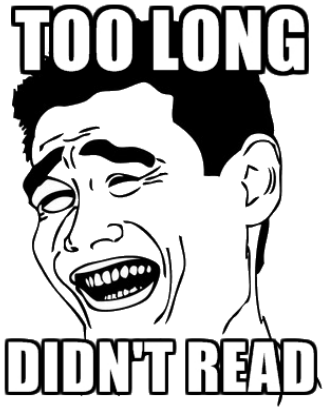
ldapsearch

- Options
  - -b searchbase
  - -s {base|one|sub|children} #defult is sub
  - -D binddn
  - -x #Use simple authentication instead of SASL.
  - -W #pas[illegible]uthentication
  - -H ldapuri
- ldapsearch [options] filter
  - ([illegible]bject=zjlin)
  - ldapsearch -H ldap://ldap.nap.nctucs.net -D “cn=zjlin,dc=nap,dc=nctucs,dc=net” -b “dc=nap,dc=nctucs,dc=net” -s one
- man ldapsearch



ldap.conf

- `ldapsearch -H ldap://ldap.nap.nctucs.net -b “dc=nap,dc=nctucs,dc=net” cn=zjlin`



- Edit /usr/local/etc/openldap/ldap.conf

```
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
BASE    dc=nap,dc=nctucs,dc=net
URI     ldaps://ldap.nap.nctucs.net
```

=> ldapsearch -x “cn=zjlin”

ldapsearch - searchbase vs filter

- Seach by dn

```
# ldapsearch dn='cn=zjlin,dc=nap,dc=nctucs,dc=net'
```

  - Not work!

- Use search base

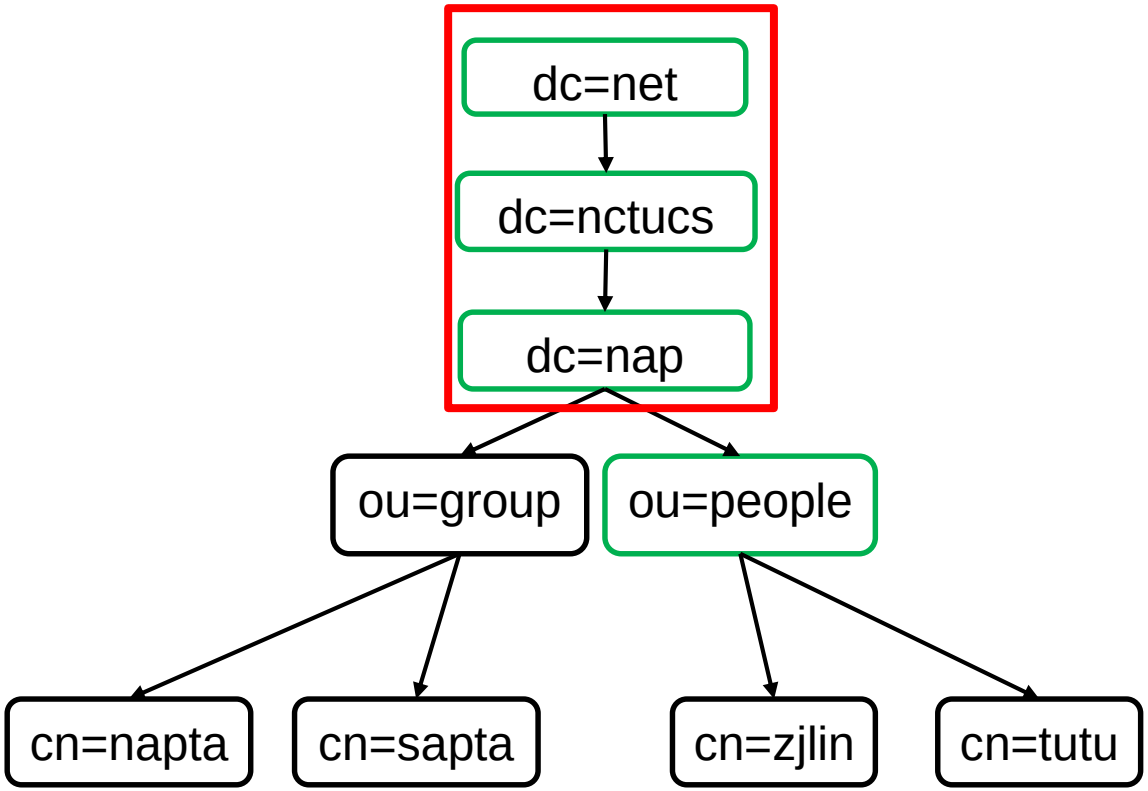
```
# ldapsearch -b 'cn=zjlin,dc=nap,dc=nctucs,dc=net' -s base
```

  - It's works!

- Why?
  - You have get full dn, don't need to search.

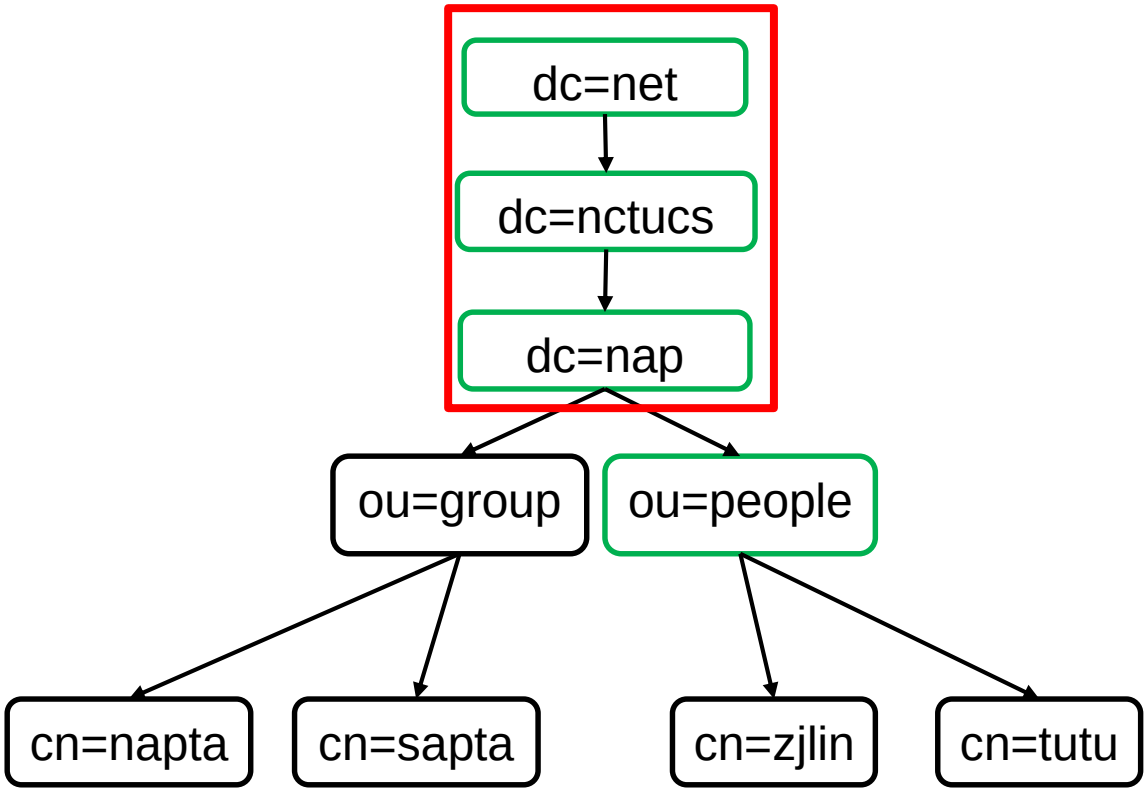
ldapsearch - searchbase vs filter

- searchbase
  - dc=nap,dc=nctucs,dc=net
  - ou=People, dc=nap,dc=nctucs,dc=net



ldapsearch - searchbase vs filter

- filter - search filter string in searchbase
  - cn=napta
  - cn=napta -> can't find



LDAP authentication

- pkg install nss-pam-ldapd
- Edit /usr/local/etc/nslcd.conf
- Edit /etc/nsswitch.conf
- Edit /etc/pam.d/system

LDAP authentication

- Edit /usr/local/etc/nslcd.conf
  - Just like ldap.conf

```
# The user and group nslcd should run as.
uid nslcd
gid nslcd
uri ldap://ldap.nap.nctucs.net
base dc=nap,dc=nctucs,dc=net
```

LDAP authentication

- Edit /etc/nsswitch.conf

https://www.freebsd.org/doc/en/articles/ldap-auth/client.html

```
# nsswitch.conf(5) - name service switch configuration file
# $FreeBSD: releng/11.1/etc/nsswitch.conf
group: files ldap
passwd: files ldap
```