

Single-Sign-On (SSO)

AD server (Active directory)

LDAP *server*

Lightweight Directory Access Protocol

tsaimh (2024-2025)
wangth (2023)

國立陽明交通大學資工系資訊中心

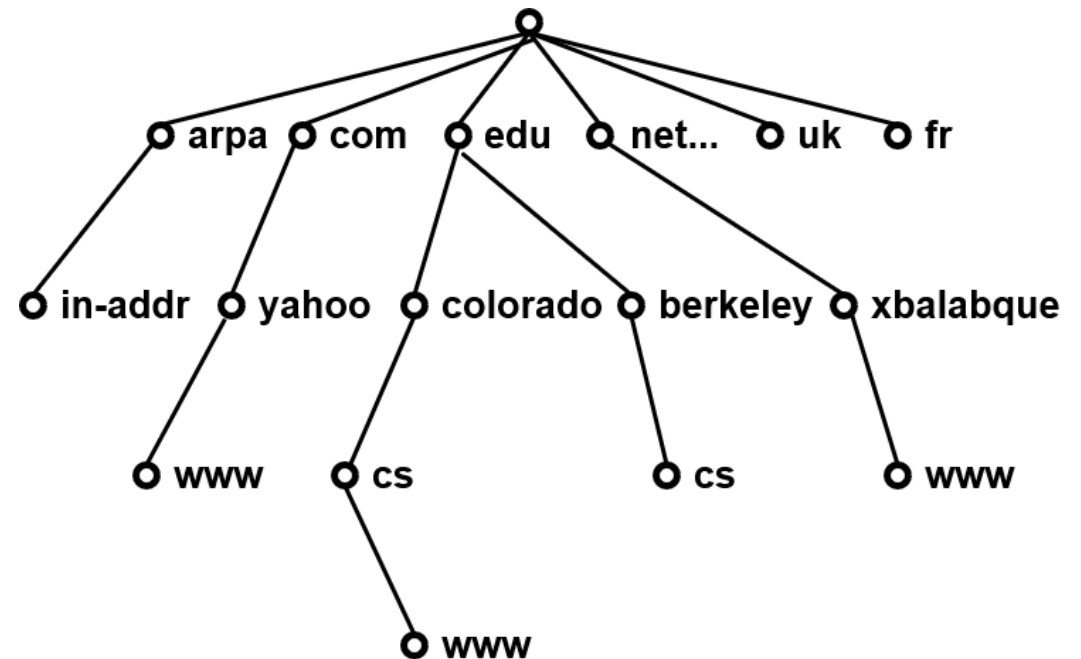
Information Technology Center of Department of Computer Science, NYCU

What is Directory Service? $\left\langle \Rightarrow \right\rangle$ DBMS v.s.

□ What is Directory Service (目錄服務) \Rightarrow 常 read 極少 write

- Highly optimized for reads
- Implements a distributed model for storing information
- Can extend the type of information it stores
- Has advanced search capabilities
- Has loosely consistent replication among directory servers

□ Domain Name Service



What is LDAP?

unix NIS (network information service) \Leftrightarrow samba

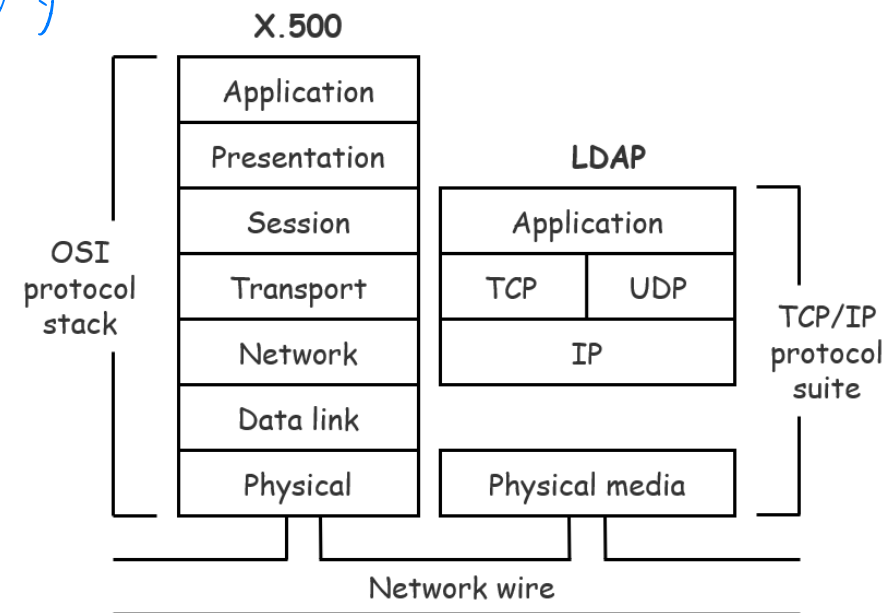
\rightarrow IETF RFC

□ The **Lightweight Directory Access Protocol (LDAP)** is an Internet protocol for **accessing distributed directory** services that act in accordance with **X.500 data and service models**.

□ Why **LDAP** is lightweight

\rightarrow ITU 定义的

- A subset of the X.500 standard
- X.500 is based on OSI model
- LDAP is based on TCP/IP model (ldap:// uses port 389, ldaps:// uses port 636)
- LDAP omits many X.500 operations that are rarely used
- Provides a smaller and simpler set of operations



RFCs for LDAP

- ❑ Lightweight Directory Access Protocol (LDAP)
 - LDAP: Technical Specification Road Map [[RFC 4510](#)]
 - LDAP: The Protocol [RFC4511]
 - LDAP: Directory Information Models [RFC4512]
 - LDAP: Authentication Methods and Security Mechanisms [RFC4513]
 - LDAP: String Representation of Distinguished Names [RFC4514]
 - LDAP: String Representation of Search Filters [RFC4515]
 - LDAP: Uniform Resource Locator [RFC4516]
 - LDAP: Syntaxes and Matching Rules [RFC4517]
 - LDAP: Internationalized String Preparation [RFC4518]
 - LDAP: Schema for User Applications [RFC4519]

LDAP Directory Information Tree (DIT)

dc: domain component

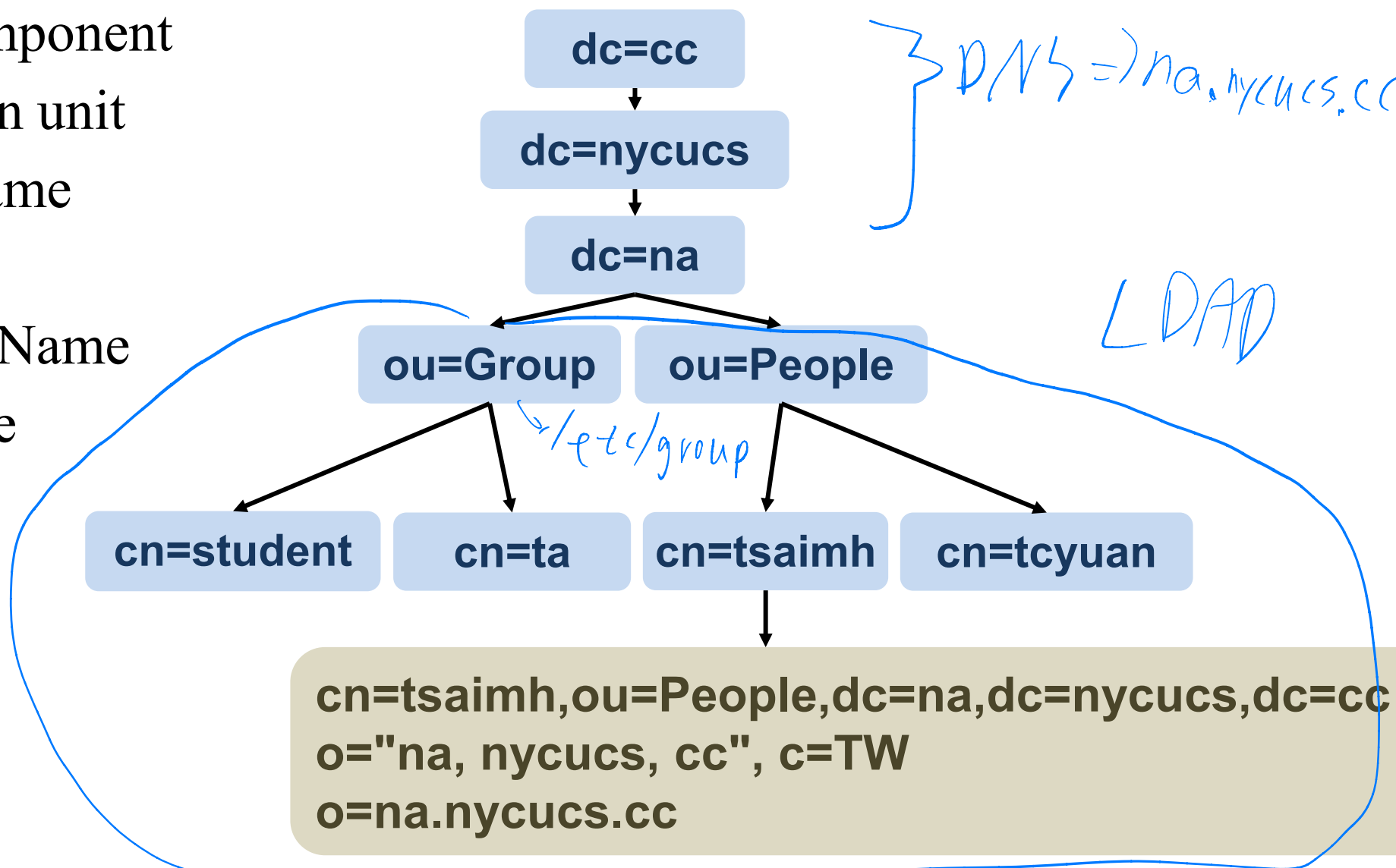
ou: organization unit

cn: common name

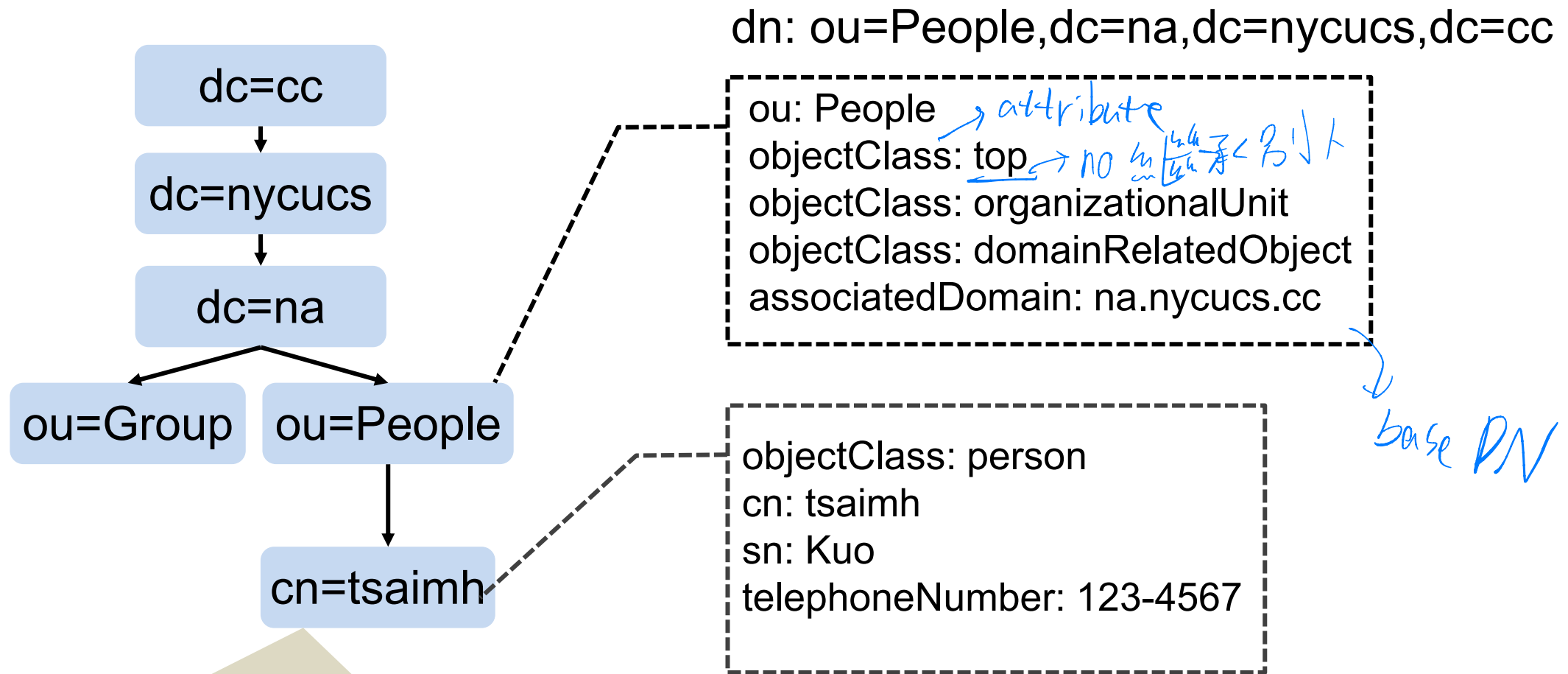
↳ attribute

o: organizationName

c: countryName



LDAP Directory Information Tree (DIT)



DN (distinguished name):
`cn=tsaimh,ou=People,dc=na,dc=nycucs,dc=cc`

absolute path

RDN: Relative Distinguished Name → relative path

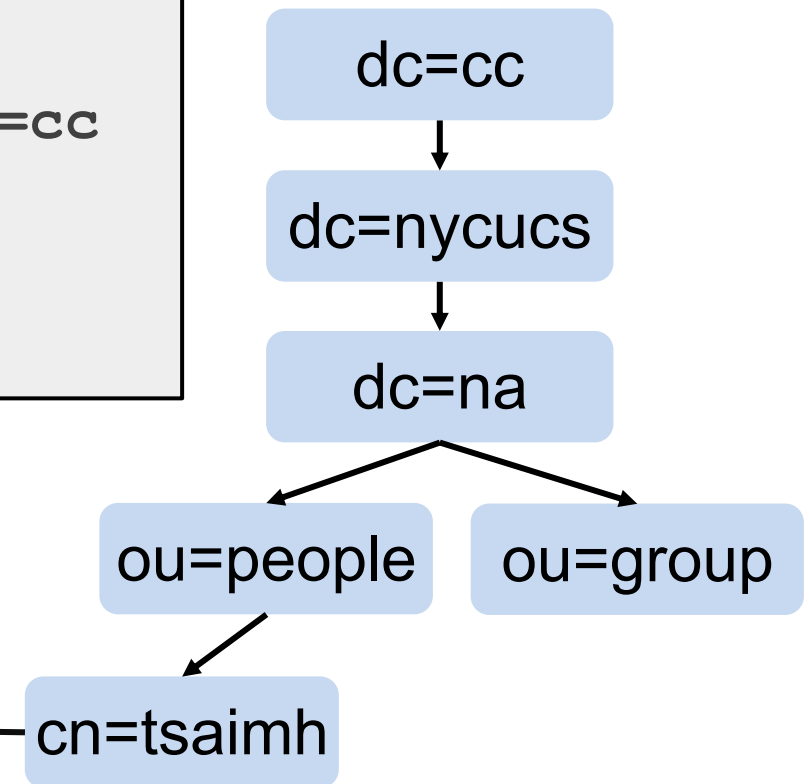
LDAPv3 Overview – LDIF (1/4)

- ❑ LDAP Interchange Format (LDIF) ⇒ OLC (online configuration)
 - 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 ⇒ each line, attribute: value
 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 (2/4)

□ Sample LDIF

```
# A sample entry
# Format: <Attribute>: <Value>
dn: cn=tsaimh,ou=people,dc=na,dc=nycucs,dc=cc
objectClass: person
cn: tsaimh
telephoneNumber: 123-4567
```



LDAPv3 Overview – LDIF (3/4)

❑ Sample LDIF – Modify one DN

Modify one DN

```
# Modify user info
dn: cn=tsaimh,ou=people,dc=na,dc=nycucs,dc=cc
changetype: modify
add: description
description: NA TA
-
replace: telephoneNumber
telephoneNumber: 0987654321
```

```
objectClass: person
cn: tsaimh
sn: abc
telephoneNumber : 123-4567
```

```
objectClass: person
cn: tsaimh
sn: abc
description : NA TA
telephoneNumber : 0987654321
```

LDAPv3 Overview – LDIF (4/4)

❑ Sample LDIF – Modify more than one DN

```
# Modify user info
dn: cn=tsaimh,ou=people,dc=na,dc=nycucs,dc=cc
changetype: modify
add: description
description: NA TA

```

```
dn: cn=wangth,ou=people,dc=na,dc=nycucs,dc=cc
changetype: modify
add: description
description: NA TA
```

Modify multiple DN



LDAPv3 Overview – objectClass

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

⇒ free bsd

→ OID

↳ default support

```
objectclass ( 2.5.6.6 NAME 'person'  
  DESC 'RFC 4519: 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 ")"

white space

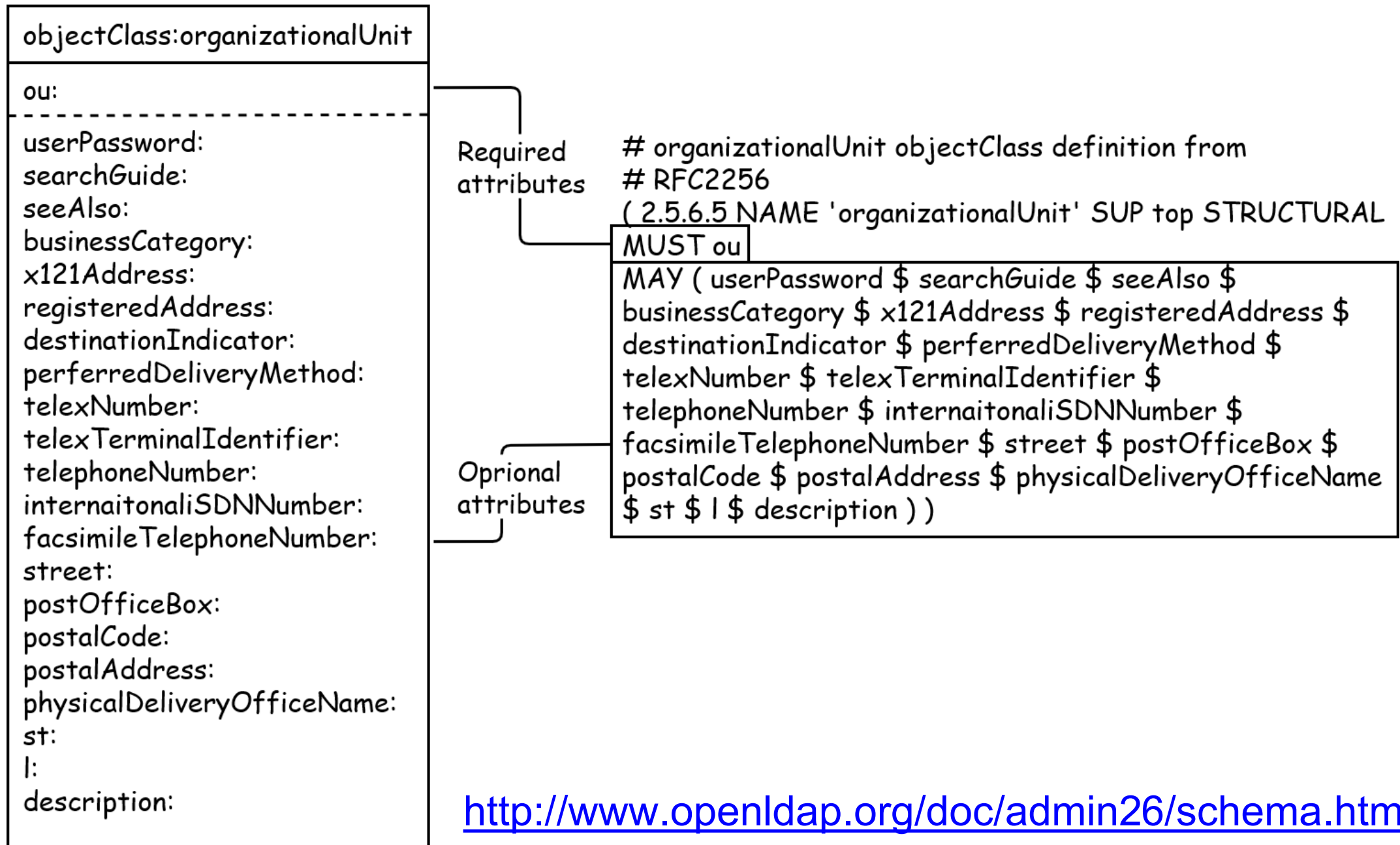
ASN.1

parent class
super class

用其他OID包含的OID内容

<http://www.openldap.org/doc/admin26/schema.html>

LDAPv3 Overview – objectClass (Cont.)



LDAPv3 Overview – Attribute

→ E.512, E.164

```
Attributetype ( 2.5.4.20 NAME `telephoneNumber'  
DESC `RFC2256: Telephone Number'  
Matching Rules EQUALITY telephoneNumberMatch  
SUBSTR telephobeNumberSubstringsMatch  
Types SYNTAX 1.3.6.1.4.1.1466.115.121.1.50{32} )
```

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	arbitrary octets

Server should support values of this length

<https://www.openldap.org/doc/admin26/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



An open source implementation of the Lightweight
Directory Access Protocol

國立陽明交通大學資工系資訊中心

Information Technology Center of Department of Computer Science, NYCU

Install OpenLDAP on Linux

❑ Installation

- `sudo apt install slapd`
- `systemctl restart packagekit.service`

❑ Check if slapd is listening port 389

- `sudo netstat -tulnp | grep slapd`

❑ Configure slapd

- `sudo dpkg-reconfigure slapd`

```
Configuring slapd
-----
If you enable this option, no initial configuration or database will be created for you.
Omit OpenLDAP server configuration?
<Yes>                                <No>
```

Install OpenLDAP on Linux (cont.)

Configuring slapd

The DNS domain name is used to construct the base DN of the LDAP directory. For example, 'foo.example.org' will create the directory with 'dc=foo, dc=example, dc=org' as base DN.

DNS domain name:

imslab.org

<Ok>

Configuring slapd

Please enter the name of the organization to use in the base DN of your LDAP directory.

Organization name:

nasa

<Ok>

```
$ sudo slapcat
```

```
dn: dc=imslab,dc=org
```

```
objectClass: top
```

```
objectClass: dcObject
```

```
objectClass: organization
```

```
o: nasa
```

```
dc: imslab
```

```
structuralObjectClass: organization
```

```
entryUUID: 7105f58c-babc-103f-8a15-1305dfe8534f
```

```
creatorsName: cn=admin,dc=imslab,dc=org
```

```
createTimestamp: 20250501094312Z
```

```
entryCSN:
```

```
20250501094312.060492Z#000000#000#000000
```

```
modifiersName: cn=admin,dc=imslab,dc=org
```

```
modifyTimestamp: 20250501094312Z
```

OpenLDAP on FreeBSD

❑ Three main components

- `slapd` – stand-alone LDAP daemon and associated modules and tools
- libraries implementing the LDAP protocol and ASN.1 Basic Encoding Rules (BER)
- client software: `ldapsearch`, `ldapadd`, `ldapdelete`, and others

❑ Installation

- `pkg install openldap26-server`
- `cd /usr/ports/net/openldap26-server; make install clean`

❑ `slapd.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.

slapd.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

database mdb
maxsize 1073741824
suffix "dc=na,dc=nycucs,dc=cc"
rootdn "cn=Manager,dc=na,dc=nycucs,dc=cc"
rootpw <generated by slappasswd> => hash value
directory /var/db/openldap-data

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

Directory ACL

```
# access to <what> [ by <who> [<accesslevel>] [<control>] ]+
access to dn.exact="cn=Manager,dc=na,dc=nycucs,dc=cc"
    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=na,dc=nycucs,dc=cc" write
    by * none

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

Handwritten annotations:

- A blue arrow points from the `by self write` line to the `by anonymous auth` line.
- A blue box highlights the `cn=Manager,dc=na,dc=nycucs,dc=cc` part of the `by dn.base="..."` line.
- A blue arrow points from the box to the handwritten text `admin`.

If one access directive is more specific than another in terms of the entries it selects, it should appear first in the configuration

Directory ACL

<http://www.openldap.org/doc/admin26/access-control.html>

□ Access Entity Specifiers (Who)

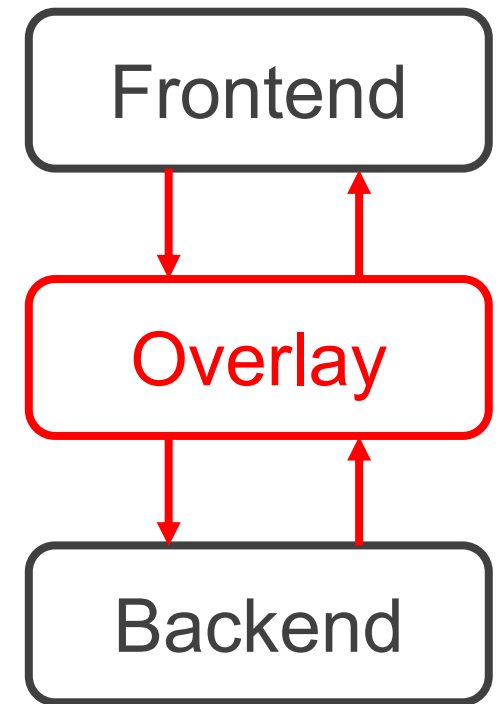
Specifier	Entities
*	All, including anonymous and authenticated users
anonymous	Anonymous (non-authenticated) users
users	Authenticated users
self	User associated with target entry
dn[.<basic-style>]=<regex>	Users matching a regular expression
dn.<scope-style>=<DN>	Users within scope of a DN

□ Access Levels

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

Overlays

- ❑ 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

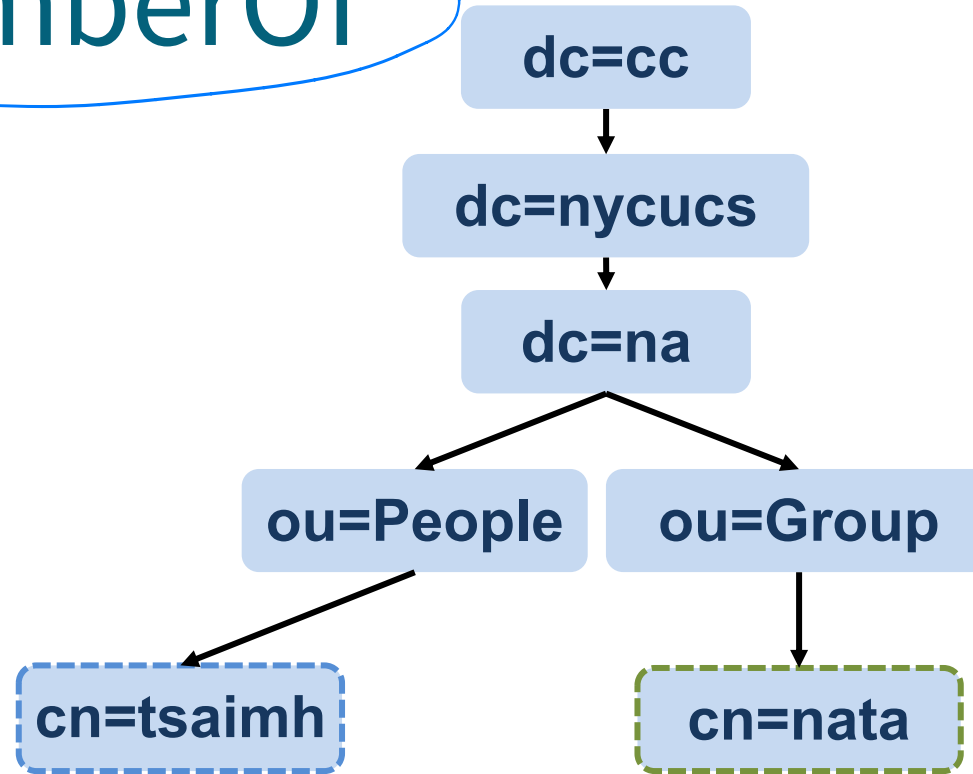


<https://www.openldap.org/doc/admin26/overlays.html>

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

Overlays - memberOf

□ Membership



objectClass: posixGroup
objectClass: top
objectClass: posixAccount
cn: tsaimh
gidNumber: 1234

objectClass: posixGroup
objectClass: top
cn: nata
displayName: nata
description: Domain Unix group
gidNumber: 1234

Overlays – 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
+ [ ] BLOCKUPS     With reverse lookup of client hostnames
```

<https://www.openldap.org/doc/admin26/overlays.html>

Overlays – memberOf

- ❑ Edit /usr/local/etc/openldap/slapd.conf

```
# MemberOf  
Overlay memberof
```

- ❑ restart slapd
- ❑ Query Result

```
dn: cn=nata,ou=MemberGroup,dc=na,dc=nycucs,dc=cc  
objectclass: groupOfNames  
cn: nata  
member: cn=tsaimh,ou=People,dc=na,dc=nycucs,dc=cc
```

<https://www.openldap.org/doc/admin26/overlays.html>

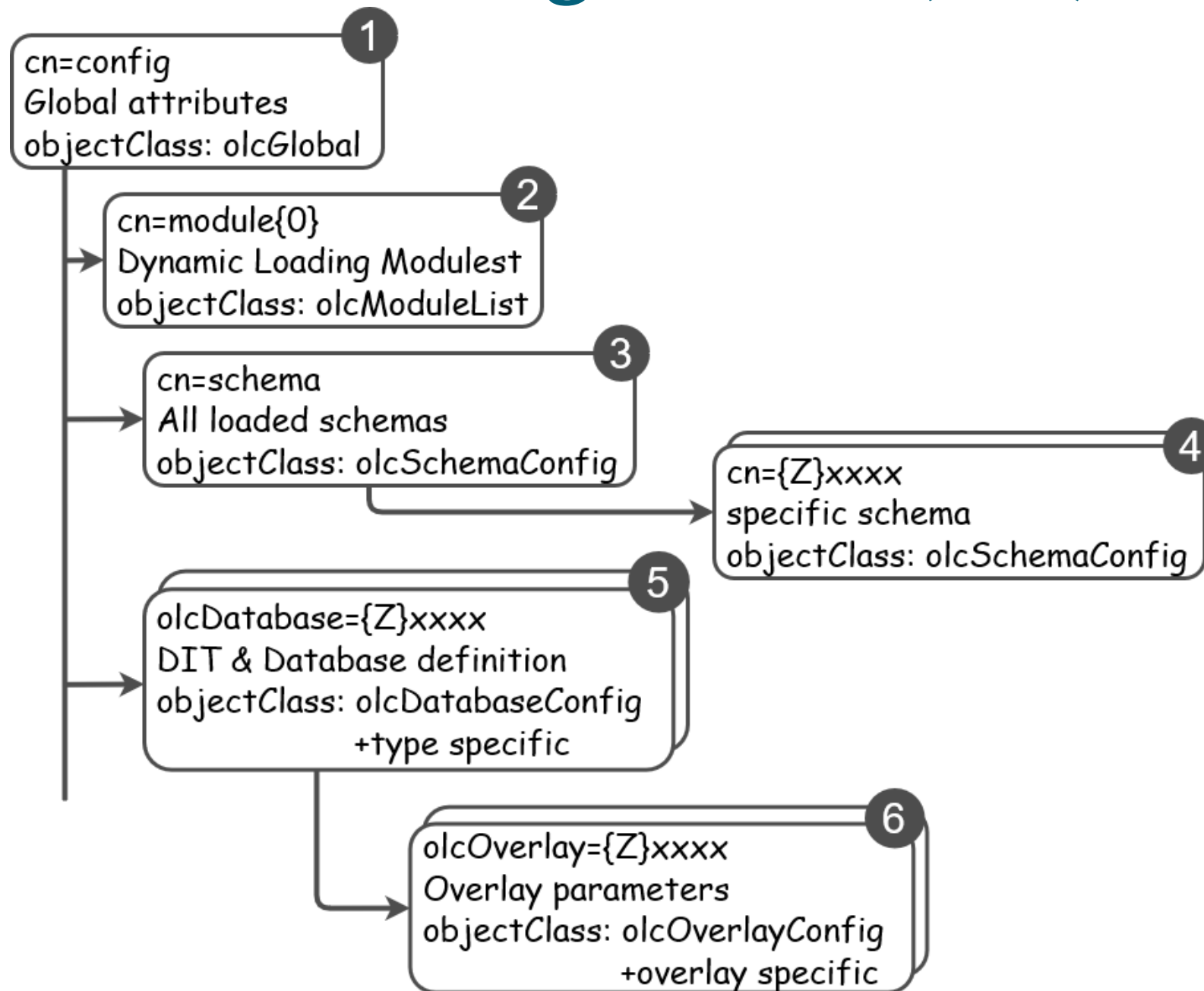
OLC – Online Configuration (1/3)

- ❑ OpenLDAP 2.3 and later have transitioned to using a dynamic runtime configuration engine
- ❑ Uses a configuration DIT to control the operational configuration
- ❑ Modifying entries in this DIT immediate changes to slapd's operational behavior
- ❑ Note: Configuration changes should be performed via LDAP operations. **DON'T edit any of the LDIF files directly.**

<https://www.openldap.org/doc/admin26/slapdconf2.html>

<https://www.zytrax.com/books/ldap/ch6/slapd-config.html>

OLC – Online Configuration (2/3)



OLC – Online Configuration (3/3)

```
# {1}mdb, config
dn: olcDatabase={1}mdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcMdbConfig
olcDatabase: {1}mdb
olcDbDirectory: /var/db/openldap-data/na
olcSuffix: dc=na,dc=nycucs,dc=cc
olcAddContentAcl: FALSE
olcLastMod: TRUE
olcMaxDerefDepth: 15
olcReadOnly: FALSE
olcRootDN: cn=Manager,dc=na,dc=nycucs,dc=cc
olcRootPW: secret
```

Enable slapd

❑ Edit /etc/rc.conf

- slapd_enable="YES"
- slapd_flags='-h "ldapi://%2fvar%2frun%2fopenldap%2fldapi/ldap://0.0.0.0/"'
- slapd_sockets="/var/run/openldap/ldapi" *⇒ for unix domain socket*

❑ service slapd start

❑ slapd runs under a non-privileged user id (by default **ldap**)

<http://www.openldap.org/doc/admin26/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 `AuthSource` 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 server to compare two values
- ❑ ldapdelete
 - This tool deletes entries from an LDAP directory

ldapsearch

□ Options

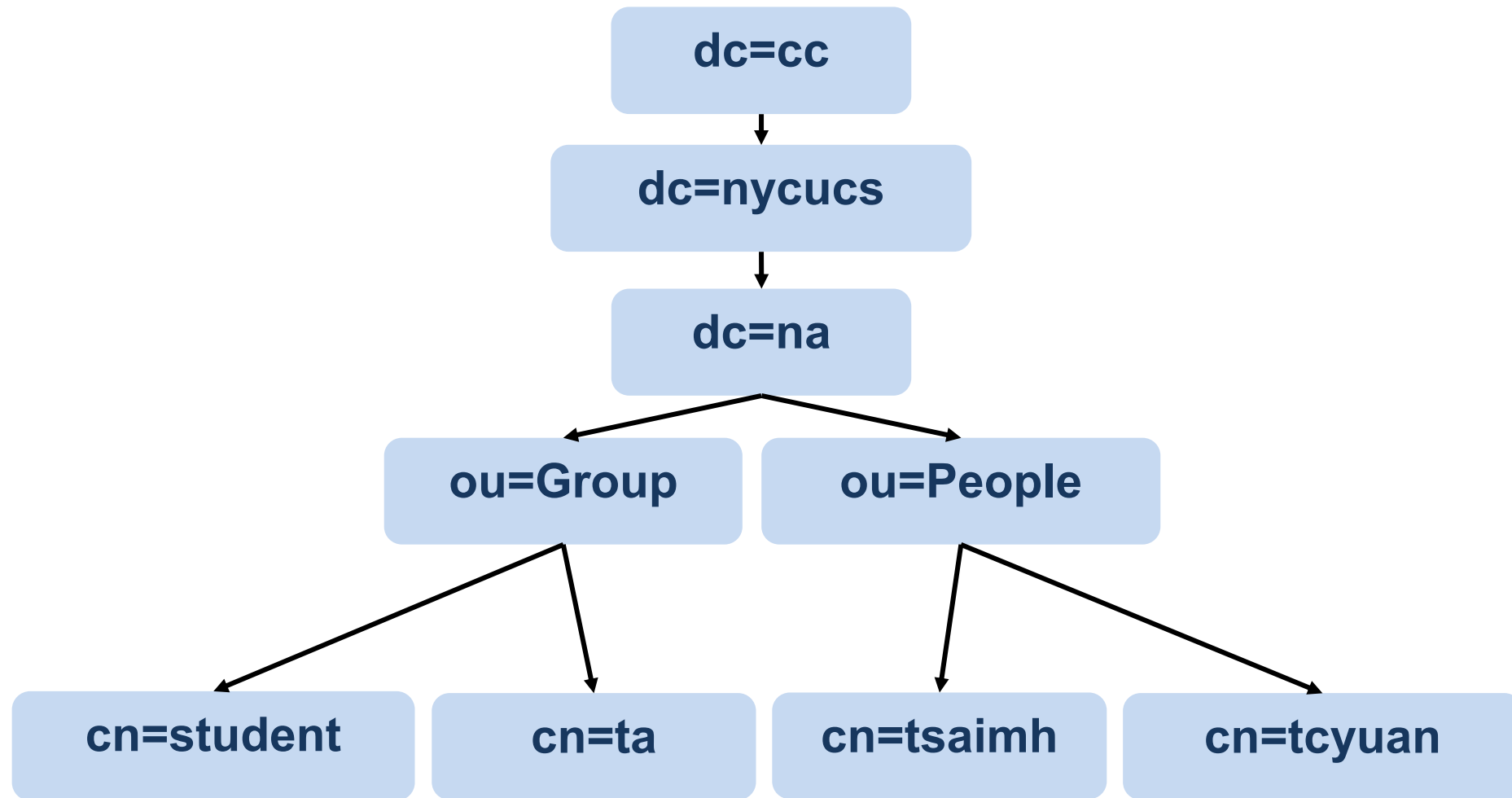
- -b searchbase
- -s {base|one|sub|children} # default is sub
- -D binddn
- -x # Use simple authentication instead of SASL
- -W # password for simple authentication
- -H ldapuri

□ ldapsearch [options] filter

- default filter, (objectClass=*)
- ldapsearch -H ldap://ldap.na.nycucs.cc
-D "cn=tsaimh,dc=na,dc=nycucs,dc=cc"
-b "dc=na,dc=nycucs,dc=cc" -s one

□ man ldapsearch

Ldapsearch (Cont.)



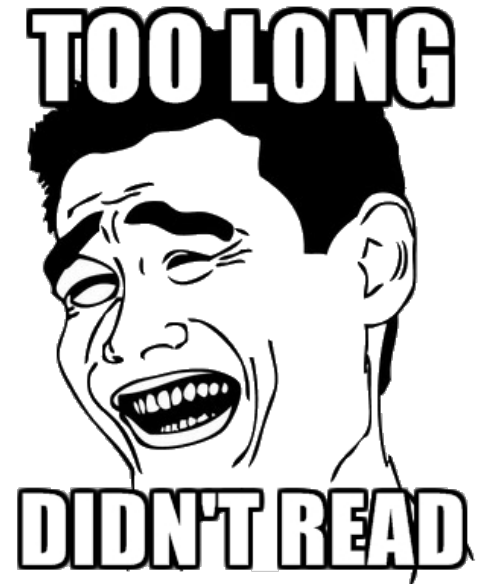
ldap.conf

❑ `ldapsearch -H ldap://ldap.na.nycucs.cc
-b "dc=na,dc=nycucs,dc=cc" cn=tsaimh`

❑ 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=na,dc=nycucs,dc=cc
URI       ldap://ldap.na.nycucs.cc
```

=> `ldapsearch -x "cn=tsaimh"`



Ldapsearch – searchbase vs. filter

❑ Search by dn

```
# ldapsearch dn="cn=tsaimhh,dc=na,dc=nycucs,dc=cc"
```

- It does not work!

❑ Use search base

```
# ldapsearch -b "cn=tsaimh,dc=na,dc=nycucs,dc=cc" -s base
```

- It works!

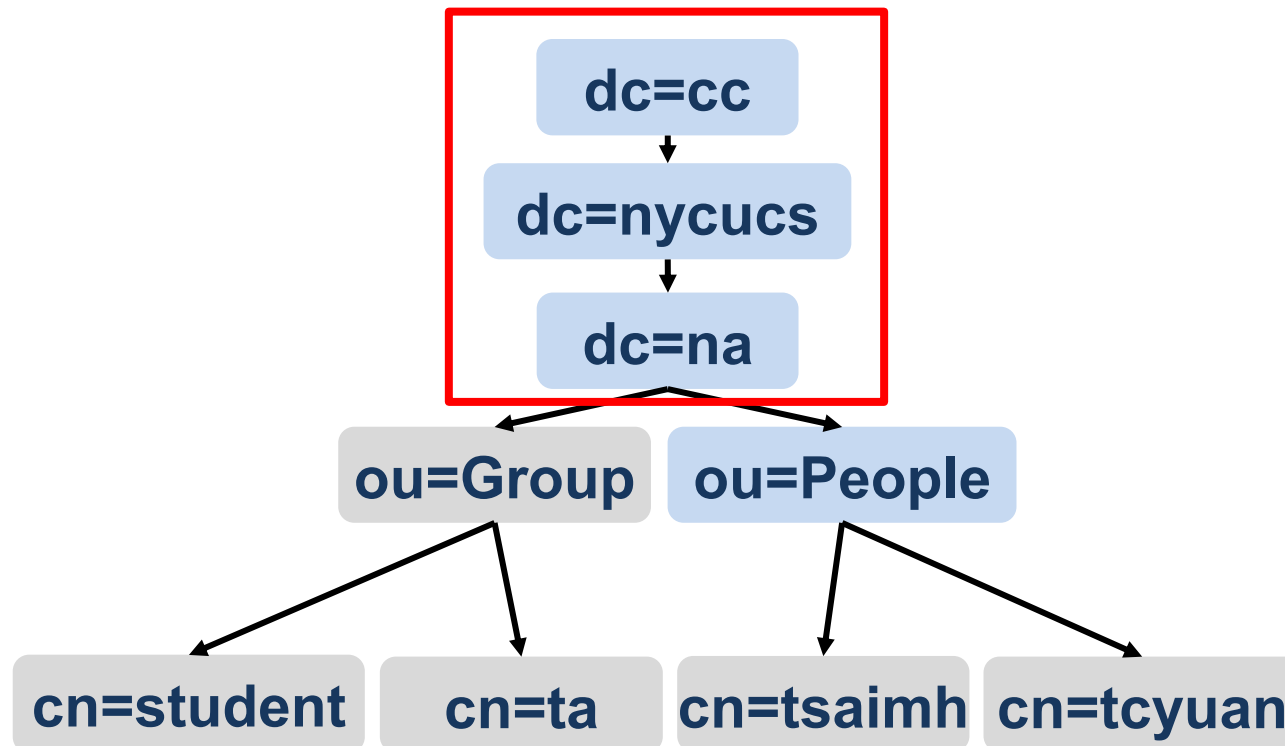
❑ Why?

- You have got full dn, don't need to search

Ldapsearch – searchbase vs. filter

□ Example

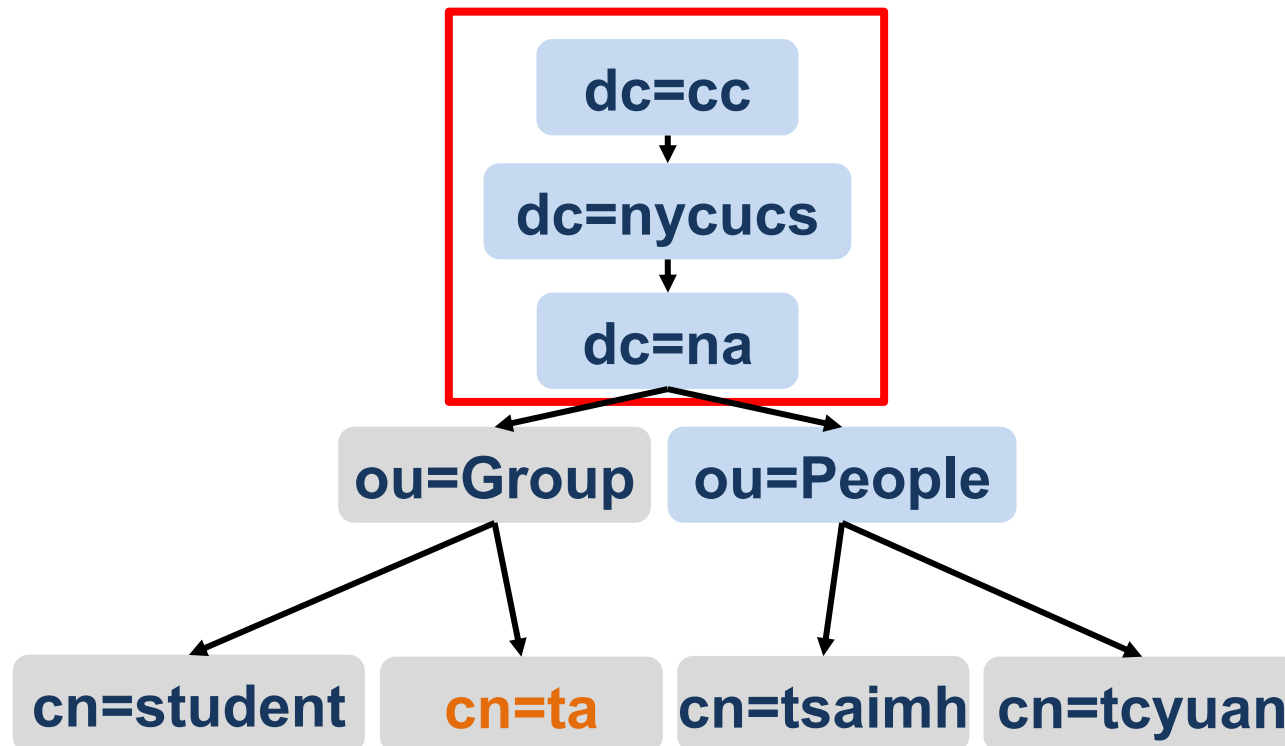
- Assume there are two kinds of searchbase
- **dc=na,dc=nycucs,dc=cc**
- **ou=People, dc=na,dc=nycucs,dc=cc**



Ldapsearch – searchbase vs. filter

□ Exatsaimh(Cont.)

- filter – search for all entries that have cn=nata
- **cn=nata**
- **cn=nata** → Can't be found, because the cn=nata is not in this subtree



LDAP Authentication

國立陽明交通大學資工系資訊中心

Information Technology Center of Department of Computer Science, NYCU

LDAP Authentication (1/3)

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

LDAP Authentication (2/3)

- ❑ 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.na.nycucs.cc  
base dc=na,dc=nycucs,dc=cc
```

LDAP Authentication (3/3)

□ 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
```

→ /etc/group
→ /etc/passwd

References

- ❑ Understanding Directory Services
 - Beth Sheresh, Doug Sheresh - Sams Publishing
- ❑ LDAP System Administration: Putting Directories to Work
 - Gerald Carter - O'Reilly Media, Inc.
- ❑ The Lightweight Directory Access Protocol: X.500 Lite
 - Timothy A. Howes
- ❑ Internet protocol suite – Wikipedia
 - https://en.wikipedia.org/wiki/Internet_protocol_suite#Comparison_of_TCP/IP_and_OSI_layering