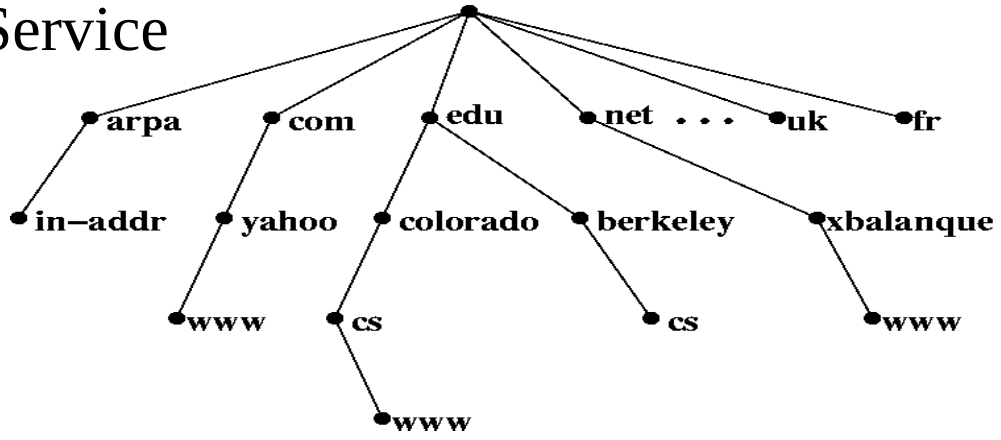
LDAP

(Lightweight Directory Access Protocol)

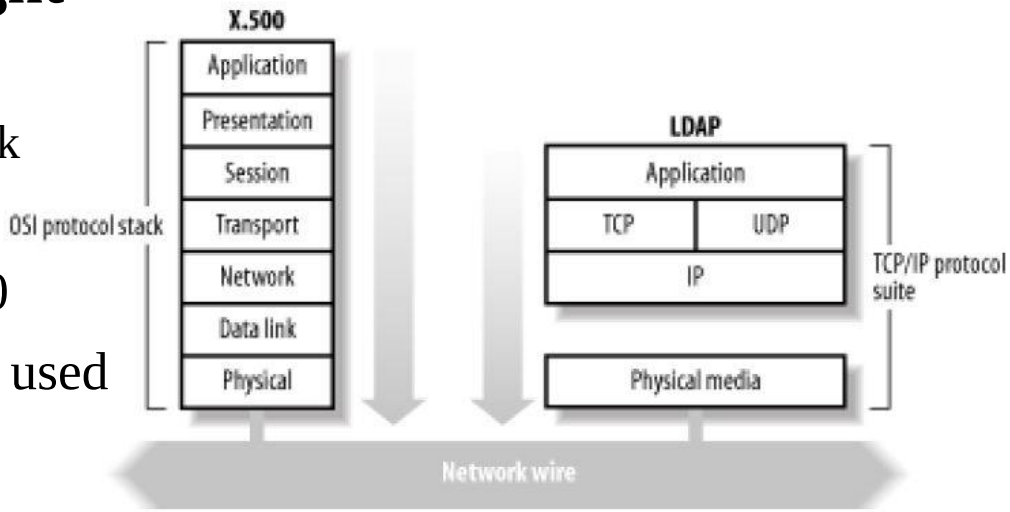
What is Directory Service

- 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 can extend the type of information stores.
  - 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**
  - 相對於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

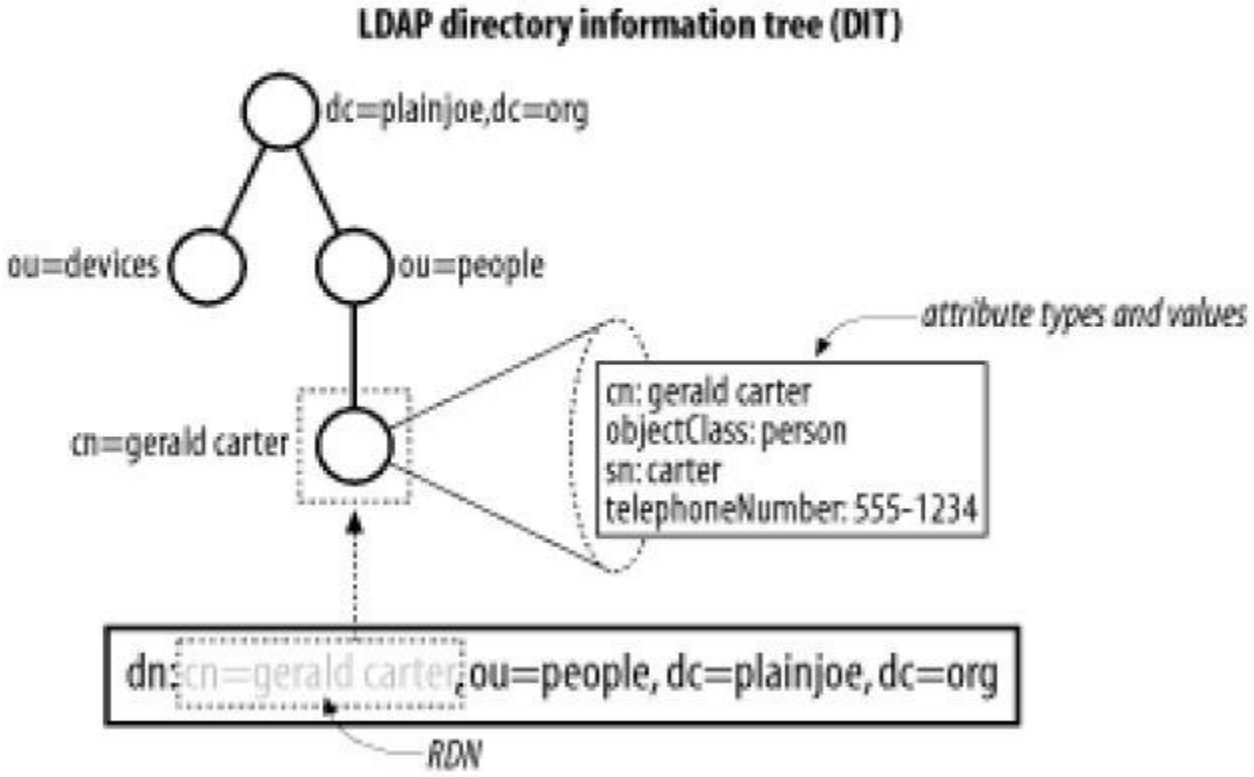


LDAP models

- RFC 2251 divides an LDAP directory into two components
  - Protocol model
  - Data model
- in *Understanding and Deploying LDAP Directory Services*, four models are defined
  - Information model
    - provides the structures and data types necessary for building an LDAP directory tree.
  - Naming model
    - defines how entries and data in the DIT are uniquely referenced.
  - Functional model
    - The LDAP protocol itself
  - Security model
    - provides a mechanism for authentication and authorization

LDAP Directory Information Tree (DIT)

Figure 1-4. Example LDAP directory tree



LDAPv3 overview – LDIF 1/2

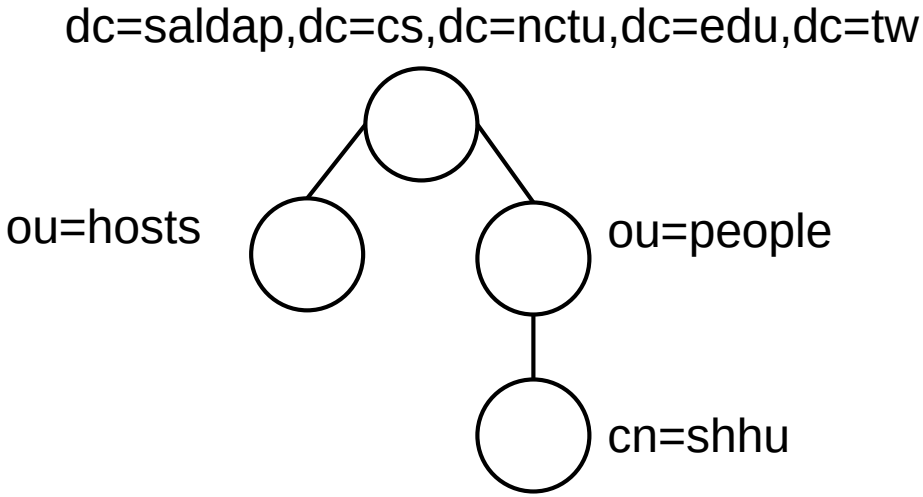
- LDAP Interchange Format (LDIF)
  - Defined in RFC 2849
  - standard text file format for storing LDAP configuration information and directory contents
  - An LDIF file is
    - A collection of entries separated from each other by blank lines
    - A mapping of attribute names to values
    - A collection 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 2/2

- Simple LDIF

```
#LDIF listing for the entry  dn: dc=saldap,dc=cs,dc=nctu,dc=edu,dc=tw
dn: dc=saldap,dc=cs,dc=nctu,dc=edu,dc=tw
objectClass: domain
dc: saldap
```

dc: domain component
DN: distinguished name
RDN: relative distinguished name
cn: common name



LDAPv3 overview – Attribute

- Attribute
  - Used to hold values

```
#LDIF listing for the entry  dn: ou=device,dc=saldap,dc=cs,dc=nctu,dc=edu,dc=tw
dn: ou=device,dc=saldap,dc=cs,dc=nctu,dc=edu,dc=tw
objectClass: organizationalUnit
ou: devices
telephoneNumber: 01234567
Description: Container for all network enabled
```

- Attribute Syntax

```
# attributetype definition for telephoneNumber
# From RFC 2256
attributetype ( 2.5.4.20 NAME 'telephoneNumber'
        EQUALITY telephoneNumberMatch
        SUBSTR telephoneNumberSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.50{32} )
```

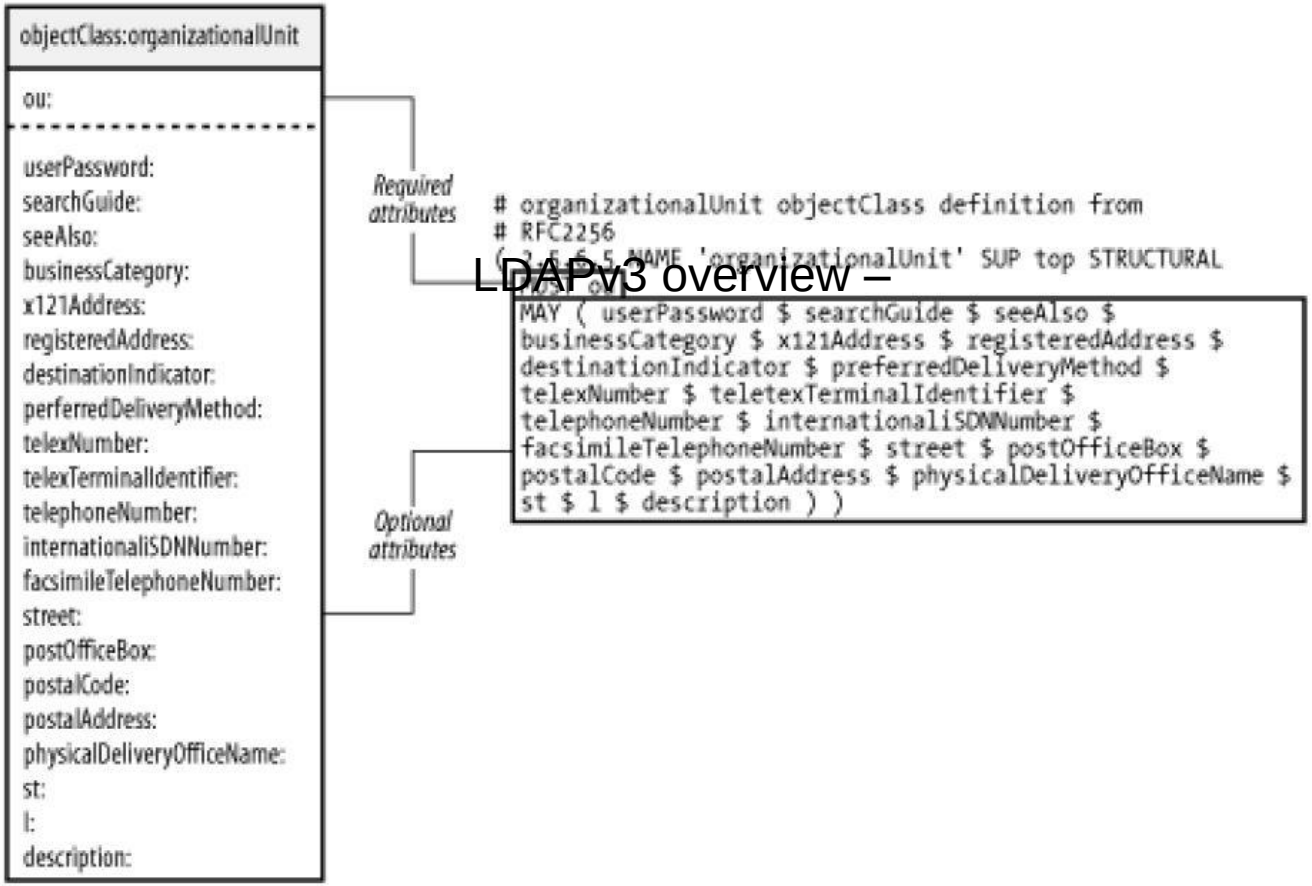
Matching rules → EQUALITY telephoneNumberMatch / SUBSTR telephoneNumberSubstringsMatch

Encoding rules → SYNTAX 1.3.6.1.4.1.1466.115.121.1.50{32}

Recommended minimum for the largest length of data

LDAPv3 overview – Attribute

- objectClass attribute



LDAPv3 overview –

LDAPv3 overview – dc attribute

- The original recommendation for dividing the X.500 namespace was based on geographic and national regions

```
dn: o=csnctu,l=Hsinchu,c=Taiwan
```

- RFC 2247 introduced a system by which LDAP directory naming contexts can be piggybacked on top of an organization's existing DNS infrastructure

LDAPv3 overview – Authentication

- Anonymous Authentication
- Simple Authentication
- Simple Authentication over SSL/TLS
  - LDAP: TCP/389
  - LDAP over ssl: TCP/636
- Simple Authentication and Security Layer (SASL)

OpenLDAP

- Install

```
# cd /usr/port/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
# Load dynamic backend modules:
modulepath      /usr/local/libexec/openldap
moduleload      back_bdb
database        bdb
suffix          “dc=saldap,dc=cs,dc=nctu,dc=edu,dc=tw"
rootdn          "cn=Manager,dc=saldap,dc=cs,dc=nctu,dc=edu,dc=tw"
rootpw          secret
directory       /var/db/openldap-data
# Indices to maintain
index   objectClass     eq
```

Directory ACL

```
access to attrs=userPassword
        by self write
        by anonymous auth
        by dn.base="cn=Manager,dc=saldap,dc=cs,dc=nctu,dc=edu,dc=tw" write
        by * none

access to attrs=englishname,birthdate
        by self write
        by users read
        by anonymous read
        by dn.base="cn=Manager, dc=saldap,dc=cs,dc=nctu,dc=edu,dc=tw" write
        by * none

access to *
        by self read
        by users read
        by anonymous read
        by dn.base="cn=Manager, dc=saldap,dc=cs,dc=nctu,dc=edu,dc=tw" write
        by * none
```

Directory ACL

Access level	Permission granted
write	Access to update attribute values (e.g., Change this telephoneNumber to 555-2345).
read	Access to read search results (e.g., Show me all the entries with a telephoneNumber of 555*).
search	Access to apply search filters (e.g., Are there any entries with a telephoneNumber of 555*).
compare	Access to compare attributes (e.g., Is your telephoneNumber 555-1234?).
auth	Access to bind (authenticate). This requires that the client send a username in the form of a DN and some type of credentials to prove his or her identity.
none	No access.

Start LDAP service

- vi /etc/rc.conf

```
# vi /etc/rc.conf
> #LDAP Server
> slapd_enable="YES"
```

- /usr/local/etc/rc.d/slapd start

Slap 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

```
# ldapsearch uid=shhu
# ldapsearch -D "uid=shhu,ou=People,dc=cs,dc=nctu,dc=edu,dc=tw" -
W uid=shhu
```

- 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

ldapmodify

- vi modify.ldif

```
dn: uid=xxx,ou=People,dc=cs,dc=nctu,dc=edu,dc=tw
changetype: modify
replace: chineseName
chineseName: 王大明
```

- ldapmodify -H ldap://ldapserver -D "cn=Manager,dc=saldap,dc=cs,dc=nctu,dc=edu,dc=tw" -W -f modify.ldif

ldapdelete

- vi delete.ldif

```
dn: uid=cccs-31407$,ou=Computers,dc=cs,dc=nctu,dc=edu,dc=tw
changetype: delete

dn: uid=cccs-31423$,ou=Computers,dc=cs,dc=nctu,dc=edu,dc=tw
changetype: delete

dn: uid=cccs-31402$,ou=Computers,dc=cs,dc=nctu,dc=edu,dc=tw
changetype: delete
```

Referance

- http://sec.cs.kent.ac.uk/x500book/ X.500
- LDAP system administration