

# Finding Information in an LDAP Directory

**Info. Tech. Svcs.**

**University of Hawaii**

**Russell Tokuyama**

**05/02/01**

University of Hawaii © 2001

# What's the phone number?

---

A scenario:

You just left a meeting and forgot to get some important information. Now, you need to call someone whose name you wrote down but don't know their office phone number or email address.

# What's the phone number?

---

- Where to look?
- What do I ask for?
- How do I ask for it?
- What will I get back?

# Where do I look?

---

- White pages (phone book)
- UH INFO - <http://www.hawaii.edu/dir/>
- An application using LDAP

# LDAP Directory

---

- DIT - directory information tree
- hierarchical - like a file system
- subtrees - groups
- search area

# What do I ask for?

---

- **Thing(s) to match**
  - All fields
  - Selected fields
  - No fields (presence, existence)

# How do I ask for it?

---

- **Host:port of LDAP server**
- **Search base**
- **Scope**
- **Search filter**
- **Attributes to return**
- **Attributes only**

# What will I get back?

---

- Zero or more entries
- Attributes
- Value(s) for each attribute present



# Demo

Someone with last name sounds like roads

```
/ou=people,o=hawaii.edu??sub?(sn~road)
```

```
/ou=people,o=hawaii.edu??sub?(sn=r*oad*)
```

# LDAP Terminology

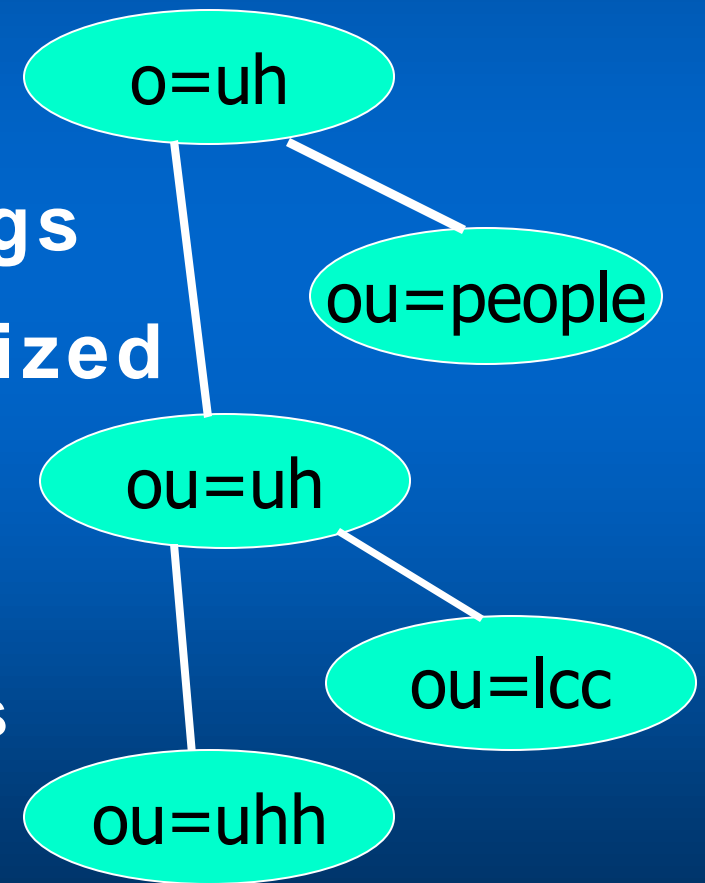
---

- **Namespace**
- **Schema**
- **Object class**
- **Attribute, Entry, Value**
- **Distinguished Name**

# LDAP Terminology

- **Namespace**

- What do you call things
- How things are organized
- Hierarchical DIT
  - Contains entries
  - Entries contain entries



# LDAP Terminology

---

- **Schema**

- **What data can be stored**
- **Object classes**
- **Attributes in the classes**
  - **Name**
  - **Type**
  - **Value**

# LDAP Terminology

---

- **Object class**
  - **Grouping of attributes**
    - required
    - optional
  - **Inheritance**
    - extend existing classes

person

orgPerson

inetOrgPerson

# LDAP Terminology

---

- **person**

- **surname**
- **common name**
- **user password (opt)**
- **phone number (opt)**
- **see also (opt)**
- **description (opt)**

person

orgPerson

inetOrgPerson

# LDAP Terminology

---

- **organizationalPerson**

- surname
- common name
- user password, phone, descr, etc. (opt)
- title, orgUnit, etc. (opt)

person

orgPerson

inetOrgPerson

# LDAP Terminology

---

- **inetOrgPerson**

- **surname**
- **common name**
- **user password, phone, descr, etc. (opt)**
- **title, orgUnit, etc. (opt)**
- **givenName, uid, mail, etc. (opt)**

```
graph TD; person --> orgPerson; orgPerson --> inetOrgPerson;
```

person

orgPerson

inetOrgPerson



# LDAP Terminology

---

- **Attribute**

- **Type (syntax)**

- **kind of information to be stored**
      - character
    - **how searched for**
      - ignore case

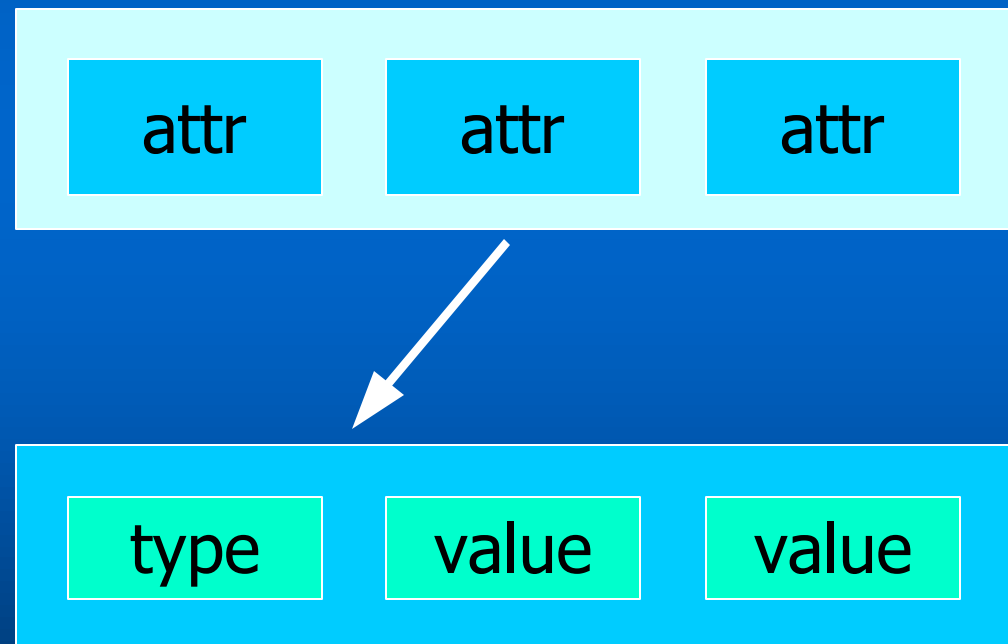
- **Value**

- **single or multiple values**

# LDAP Terminology

- **Entry**

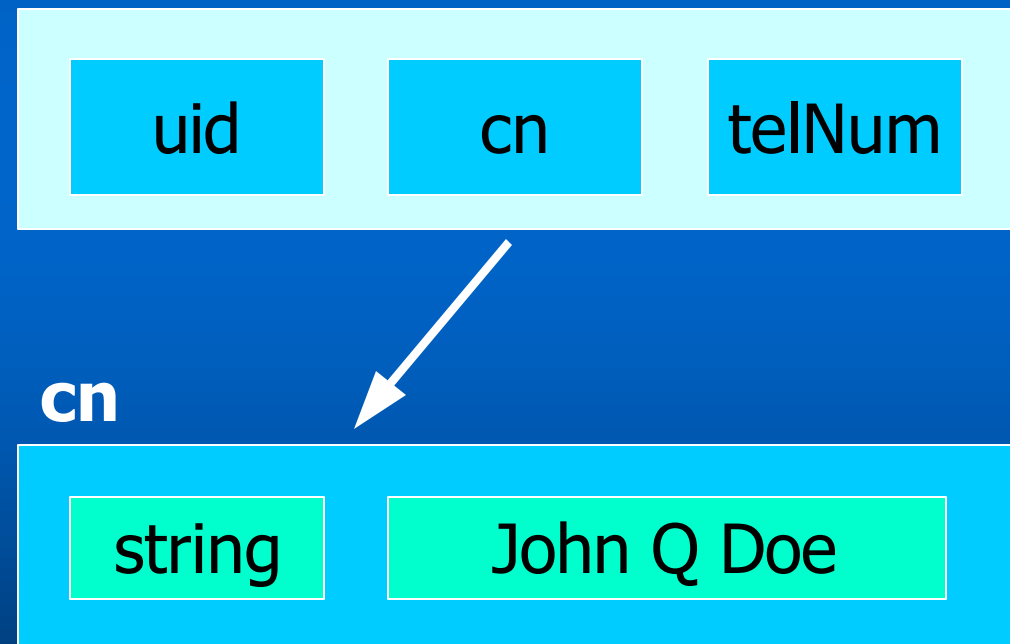
- **Attributes**
- **Types**
- **Values**



# LDAP Terminology

- **Entry**

- **Attributes**
- **Types**
- **Values**



# LDAP Terminology

---

- **Distinguished Name (DN)**
  - name of an entry
  - uniquely identifies entry
  - composed of attributes

# LDAP Terminology

- **Distinguished Name (DN)**

o=hawaii.edu

ou=People, o=hawaii.edu

ou=Groups, o=hawaii.edu

ou=UH, o=hawaii.edu

# LDAP Terminology

- **Distinguished Name (DN)**

dc=hawaii, dc=edu

ou=People, dc=hawaii, dc=edu

ou=Groups, dc=hawaii, dc=edu

ou=UH, dc=hawaii, dc=edu

# LDAP Terminology

- Distinguished Name (DN)

o=University of Hawaii, c=US

ou=People, o=University of Hawaii, c=US

ou=Groups, o=University of Hawaii, c=US

ou=UH, o=University of Hawaii, c=US

# More LDAP Terminology

---

- **Search base**
  - What part of the DIT to look in
- **Scope**
  - Base, One, Sub
- **Search filter**
  - What to use as a comparison



# More LDAP Terminology

- **Search base**

- What part of the DIT to look in

o=hawaii.edu

ou=People, o=hawaii.edu

ou=Groups, o=hawaii.edu

ou=UH, o=hawaii.edu

# More LDAP Terminology

---

- **Scope**
  - Base - main entry
  - One - main entry and immediate children
  - Sub - main entry and all descendants

# More LDAP Terminology

- **Search filter**
  - What to use as a comparison
  - One or more attributes
    - `firstname=John,`
    - `lastname=Doe,`
    - `department=Leeward CC`

# How to find it

---

- **LDAP URL (RFC 2255)**

- **host:port**
- **Search base**
- **Scope**
- **Search filter**

`ldap://host:port/base?attributes?scope?filter`

# How to find it

---

- **LDAP URL (RFC 2255)**

`ldap://host:port/base?attributes?scope?filter`

```
/ou=people,o=hawaii.edu??sub?(sn=Doe)
```

# How to find it

---

- **LDAP URL (RFC 2255)**
  - **Attributes** - default is all
  - **Scope** - default is base (main entry)

```
/ou=people,o=hawaii.edu??sub?(sn=Doe)
```

# Search Filters

---

- **Search Attribute(s)**
  - **Exact match**
  - **Approximate match**
    - **partial key**
    - **regular expression**
  - **Substring**

# Search Filters

- **Search Attribute(s)**
  - Exact match

```
(sn=Doe)
```

```
(& (sn=Doe) (givenName=John) )
```



# Search Filters

- **Search Attribute(s)**
  - Approximate match

```
(sn~road)
```

```
(& (sn~Doe) (givenName=John) )
```

# Search Filters

- **Search Attribute(s)**
  - Substring

```
(sn=do*)
```

```
(& (sn=r*oa*) (givenName=sam*) )
```

# Search Filters

- More examples

```
(& (sn=do*) (! (givenName=jo*)) )
```

```
(&(givenName=Jo*n) (|(sn=Do*)(sn=Sm*)))
```

# Attributes Returned

- All
- Only those of interest

telephone,mail,cn

o=hawaii.edu?telephone,mail,cn?sub?(sn=Doe)

# What's in LDAP?

---

- uid (ITS username)
- cn (last, first middle)
- givenName (first name)
- sn (last name)
- employeeType (faculty, staff, student)
- ou (home campus)

# What's coming next?

---

- Refine schema
- Refine data sources
- Enable more applications
- Engage more people