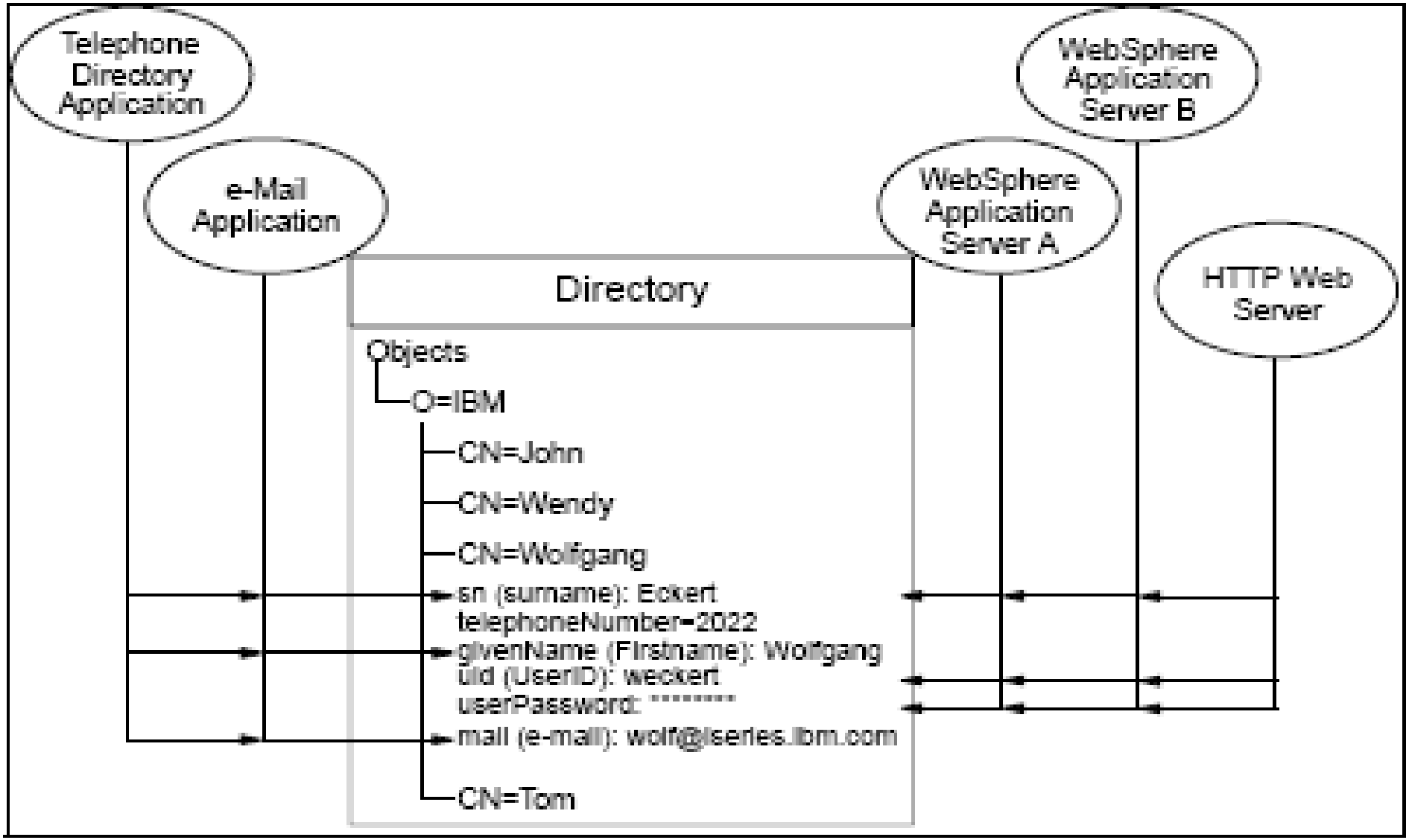
LPIC-2 TRAINING COURSE

Topic 212: Lightweight Directory Access Protocol

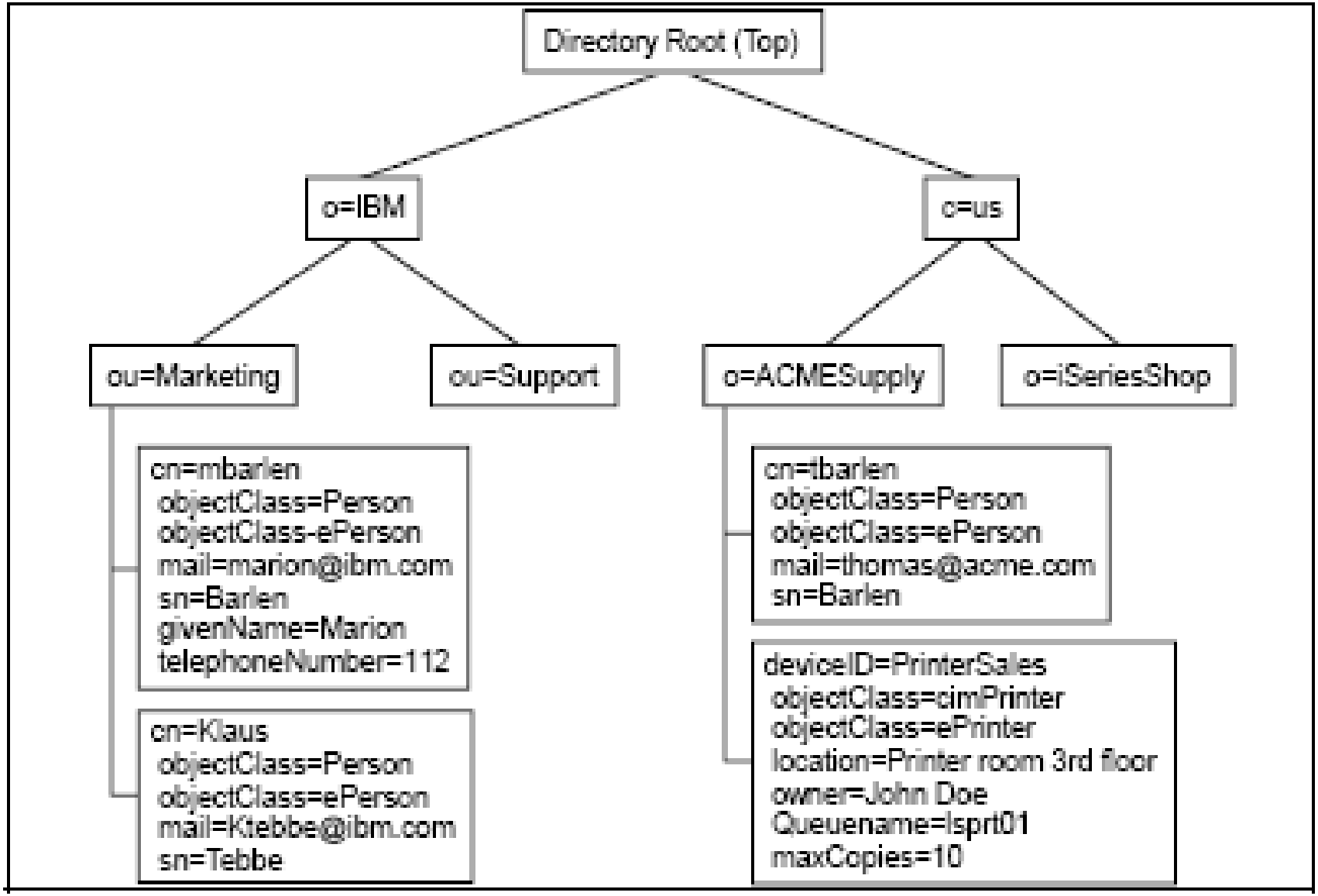
History of LDAP

- Has it's roots in X.500 (hence DAP)
- Developed initially at University of Michigan, and is now an IETF standard
- Accepted standard for Directory services, embraced by all the "big" players
- LDAP is a protocol, not a database
- Client-server based, ASN.1 encoding

Directories Advantages



Directory Structure



Distinguished Names

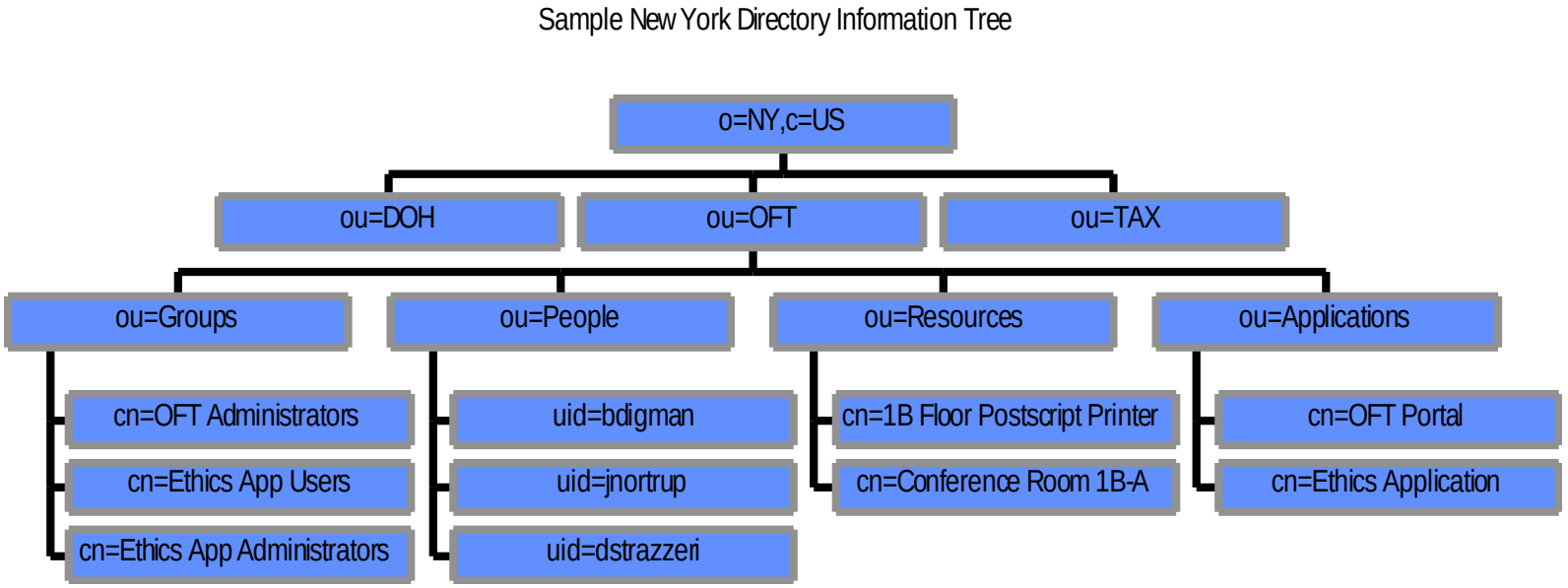
- **Each object in the LDAP directory has a DN**
  - uid=jheiss,ou=people,dc=example,dc=com
  - cn=users,ou=group,dc=example,dc=com
- **Notice that the DNS name is example.com (specified by DC=Domain Component entries) for the domain**
- **OU is organizational unit**
- **Each domain subdomain could create a tree structure in LDAP (engr.example.com, sales.example.com, pre.engr.example.com, support.engr.example.com, etc)**

LDAP Architechture

- **A typical entry serialized in LDIF:**

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 555 6789
telephoneNumber: +1 555 1234
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

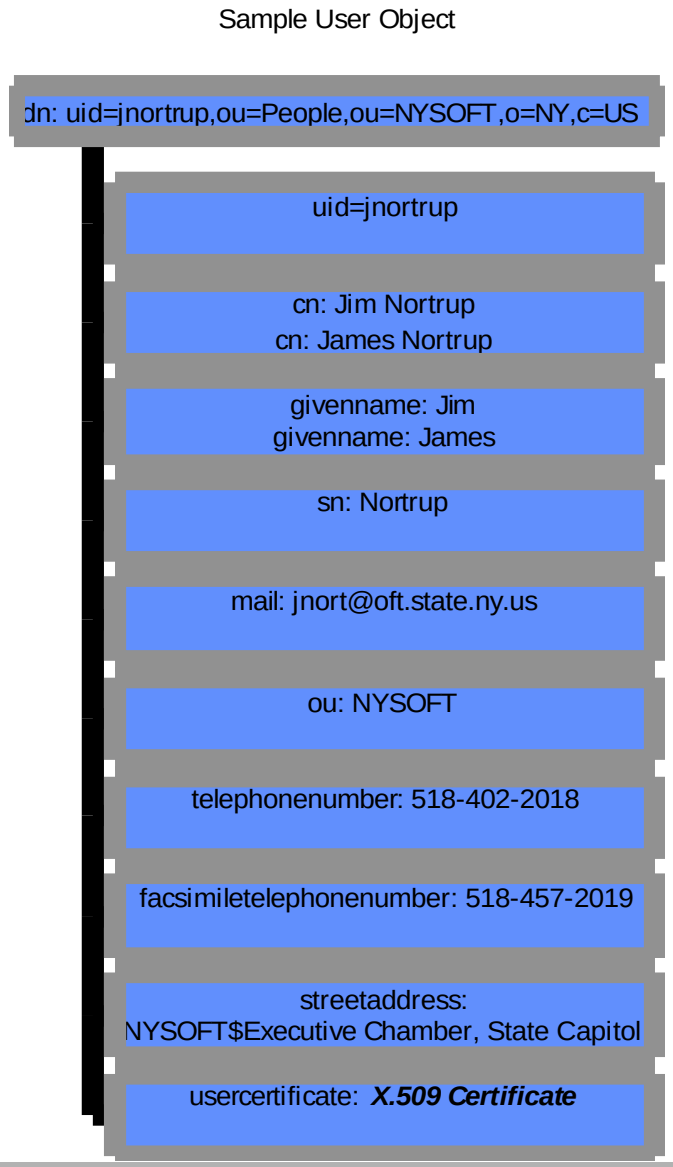
Sample DIT



- Branched by agency
- Agencies in this example have branches containing:
  - Groups which contain people
  - People in the organization
  - Resources such as printers and conference rooms
  - Applications (where application specific info. could be maintained)

Sample User Object

- **Objects contain attributes, e.g.,**
  - uid (user ID)
  - cn (common name)
  - sn (surname)
  - mail (e-mail address)
- **Attributes can be multi-valued, e.g., givenname of both James and Jim**
- **This object contains**
  - white-pages information
  - X.509 certificate for PKI



ObjectClass

- **A commonly used attribute is "objectClass".**
- **Each record represents an object, and the attributes associated with that object are defined according to *it's objectClass***
  - The value of the objectClass attribute
- **Examples of objectClass:**
  - ***organization*** (needs a ***name*** and ***address***)
  - ***person*** (needs ***name***, ***email***, ***phone*** & ***address***)
  - ***cookie*** (needs ***name***, ***cost*** & ***taste*** index)

Schemas

- **The schema defines the *attribute types* that directory entries can contain.**
- **An attribute definition includes a *syntax*, and most non-binary values in LDAPv3 use UTF-8 string syntax**
  - For example, a "mail" attribute might contain the value "user@example.com".
  - A "jpegPhoto" attribute would contain photograph(s) in binary JPEG/JFIF format.
  - A "member" attribute contains the DNs of other directory entries.
- **Attribute definitions also include whether the attribute is single-valued or multi-valued, how to search/compare the attribute.**
- **The schema defines *object classes*. Each entry must have an objectClass attribute, containing named classes defined in the schema.**
  - e.g. a person, organization or domain.
- **Server administrators can define their own schemas in addition to the standard ones.**

Basic Operations

- Search - search for and/or retrieve directory entries,
- Compare - test if a named entry contains a given attribute value
- Add a new entry
- Delete an entry
- Modify an entry
- Modify DN - move or rename an entry
- Abandon - abort a previous request
- Extended Operation - generic operation used to define other operations

Variations

- **OpenLDAP**
  - Open Source LDAP v3 implementation
    - SLAPD: Standalone server daemon
    - SLURPD: Replication daemon
    - Libraries including Java libraries
- **MS Active Directory**
  - Microsoft Directory services
  - Use LDAP & Kerberos 5
- **Netscape Directory Server**
  - Very fast, powerful ACLs
  - Cross platform
  - Standards compliant

Thank You !

BACKUP SLIDES