Course Name:

Advanced Java

Lecture 15
Topics to be covered

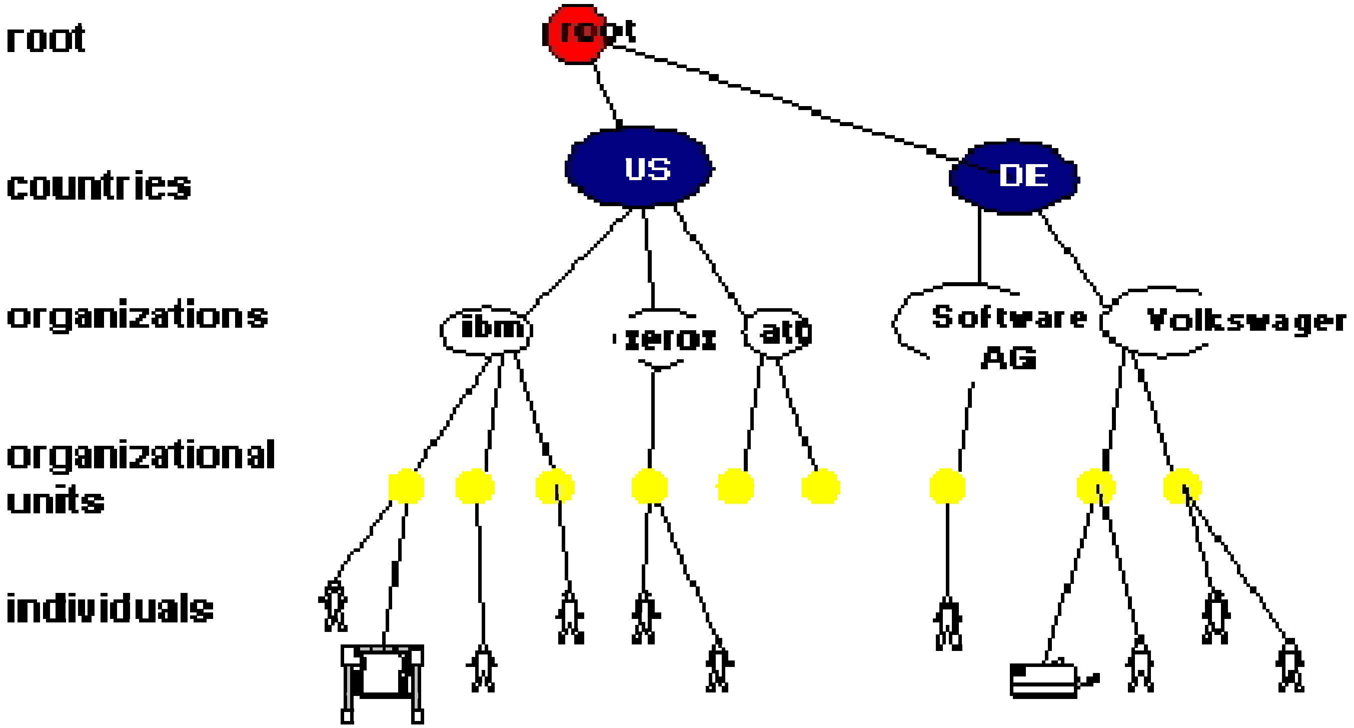
- LDAP: Background and Motivation
- Understanding LDAP
  - Information Structure
  - Naming
  - Functions/Operations
  - Security

Background and Motivation

- Increased reliance on networked computers
- Need in information
  - Functionality
  - Ease-of-Use
  - Administration (Application specific dirs)
  - Clear and consistent organization
  - Integrity
  - Confidentiality

X.500

- X.500 standard. CCITT 1988
  - Refer ISO 9594 – X.500-X.521 of 1990



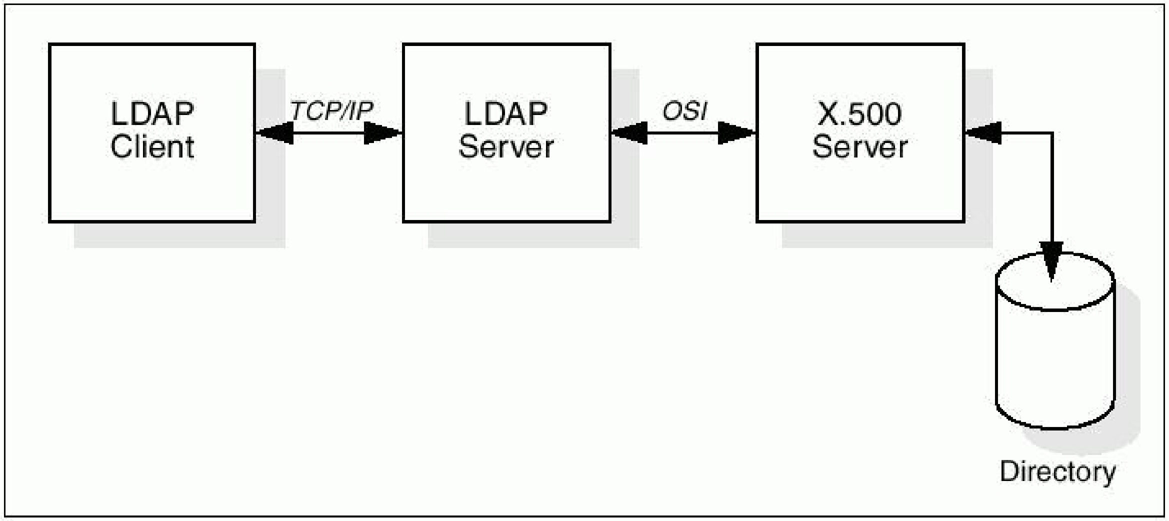
X.500

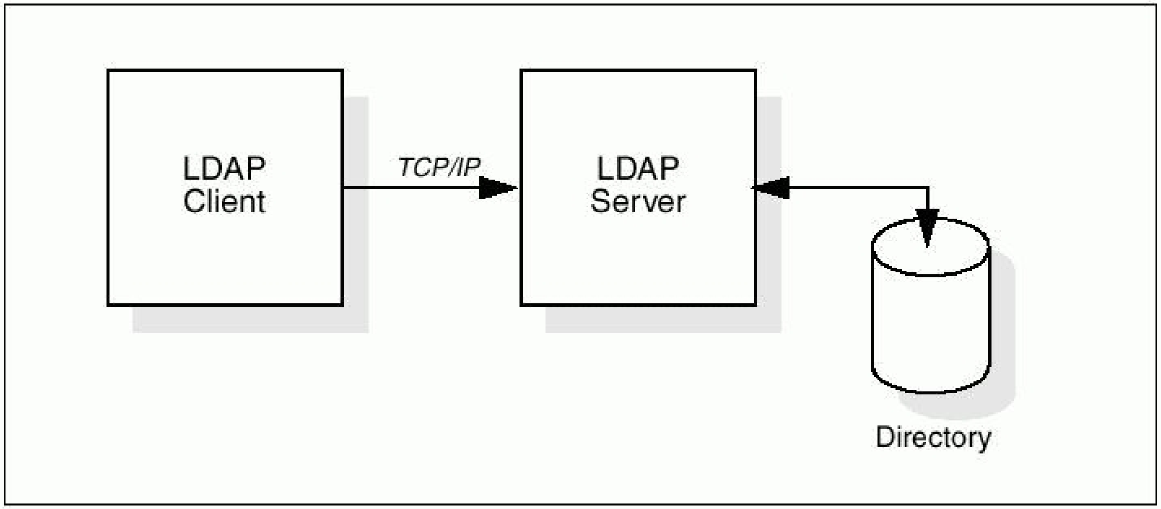
- Organizes directory entries into a hierarchical namespace
- Powerful search capabilities
- Often used for interfacing incompatible directory services
- Used DAP for c/s communication
- DAP (App. Layer) requires ENTIRE OSI stack to operate
- Too heavy for small environments

What is LDAP?

- Lightweight Directory Access Protocol
- Used to access and update information in a directory built on the X.500 model
- Specification defines the content of messages between the client and the server
- Includes operations to establish and disconnect a session from the server

LDAP Server: G/S





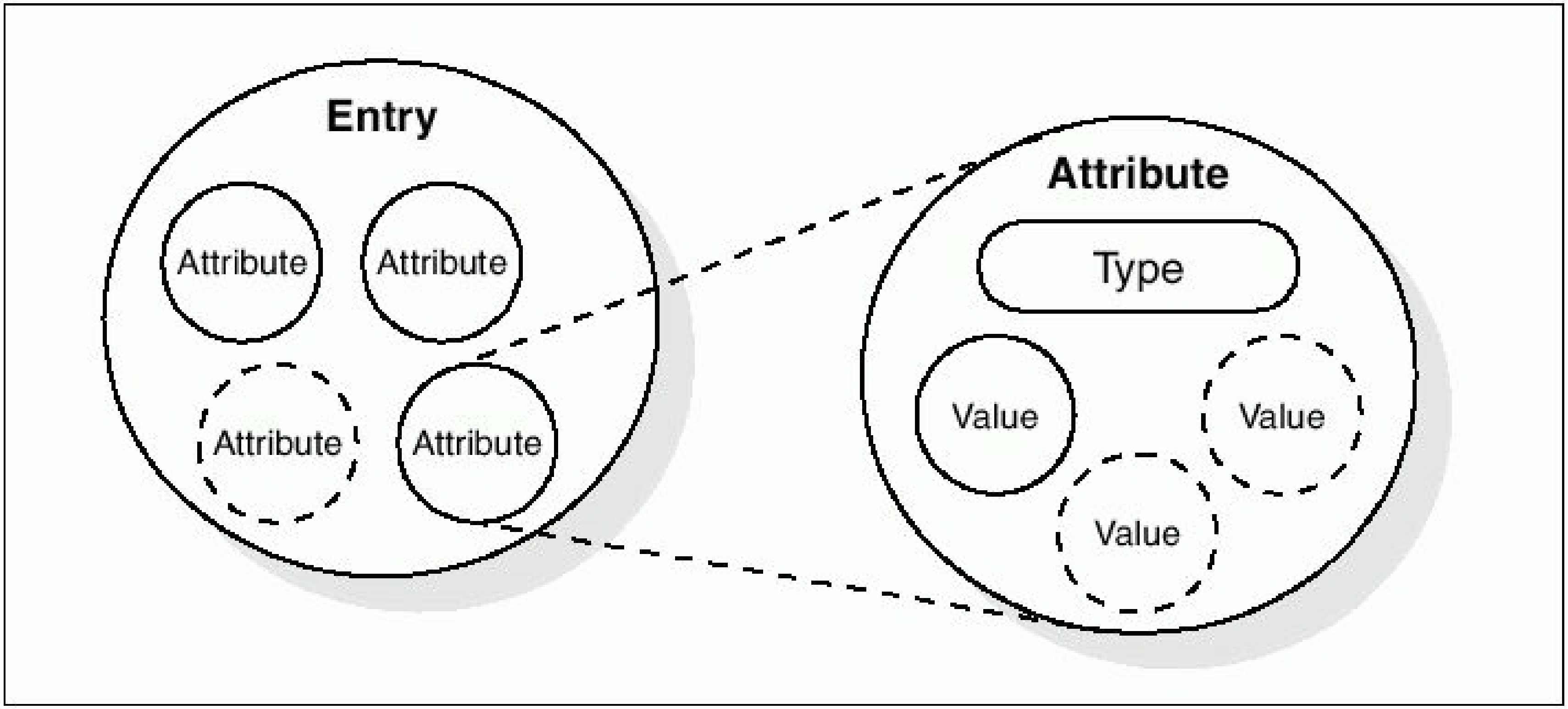
Understanding LDAP

- Lightweight alternative to DAP
- Uses TCP/IP instead of OSI stack
- Simplifies certain functions and omits others…
- Uses strings rather than DAP's ASN.1 notation to represent data.

LDAP

- **Information**
  - Structure of information stored in an LDAP directory.
- **Naming**
  - How information is organized and identified.
- **Functional / Operations**
  - Describes what operations can be performed on the information stored in an LDAP directory.
- **Security**
  - Describes how the information can be protected from unauthorized access.

LDAP Information Storage



LDAP Information Storage

- Each attribute has a type/syntax and a value
- Can define how values behave during searches/directory operations
- Syntax: bin, ces, cis, tel, dn etc.
- Usage limits: ssn – only one, jpegPhoto – 10K

LDAP Information Storage

- Each ‘entry’ describes an object (Class)
  - Person, Server, Printer etc.
- Example Entry:
  - InetOrgPerson(cn, sn, ObjectClass)
- Example Attributes:
  - cn (cis), sn (cis), telephoneNumber (tel), ou (cis), owner (dn), jpegPhoto (bin)

LDAP Naming

- DNs consist of sequence of Relative DN
  - cn=John Smith,ou=Austin,o=IBM,c=US (Leaf 2 Root) (~use \ for special)
- Directory Information Tree (DIT)
- Follow geographical or organizational scheme
- Aliases: Tree-*like,*
- Aliases can link non-leaf nodes

LDAP Naming

- Referrals: May not store entire DIT (v3)
- Referrals
  - objectClass=referral, attribute=ref, value=LDAPurl
- Implementation differs
  - Refferals/Chaining (vendor)
    - RFC 1777: server chaining is expected.

LDAP Naming

- Schema
  - Defines what object classes allowed
  - Where they are stored
  - What attributes they have (objectClass)
  - Which attributes are optional (objectClass)
  - Type/syntax of each attribute (objectClass)
- Query server for info: zero-length DN
- LDAP schema must be readable by the client

LDAP Functions/Operations

- Authentication
  - BIND/UNBIND
  - ABANDON
- Query
  - Search
  - Compare entry
- Update
  - Add an entry
  - Delete an entry (Only Leaf nodes, no aliases)
  - Modify an entry, Modify DN/RDN