IBM eServer™ iSeries™

Session: 420033

Overview of LDAP and IBM Directory Server

Beth L. Hoffman

Agenda

- Directory Overview
  - Basic Directory Example
  - Benefits of a Directory
- Uses of a Directory
  - Example Middleware and Application Use
- Directory Concepts
  - Terminology
  - Functions
  - LDAP Overview
- IBM Directory Server
  - Product Features
  - iSeries Features
  - What's New in V5R2
- Planning a New Directory

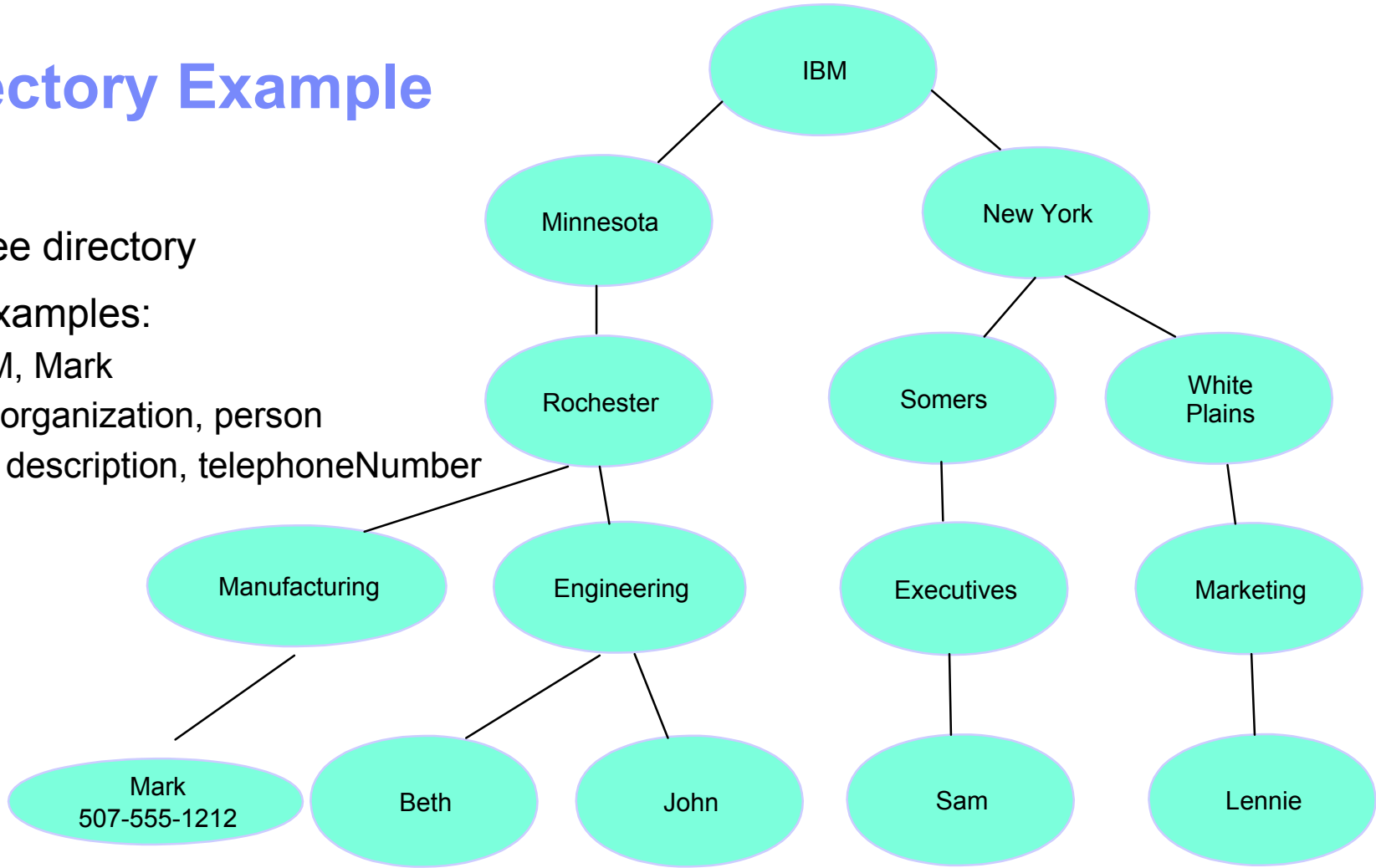
Directory Overview

Directory Information Model

- A directory is:
  - a **repository** that enables
  - sharing **commonly accessed data** across an enterprise by
  - using a **standard access protocol**
- LDAP is:
  - an open industry standard that defines the method for accessing the data
  - **L**ightweight **D**irectory **A**ccess **P**rotocol
- Examples:
  - a city telephone directory
  - a library card catalog
  - an employee organizational chart

Basic Directory Example

- IBM employee directory
- Entry data examples:
  - Name: IBM, Mark
  - Structure: organization, person
  - Attributes: description, telephoneNumber



Directory Data

How does data get into the directory?

- Add entries manually one at a time using commands
- Import data using an LDIF file
  - Manually type the contents of the file
  - Automatically create it from searching another directory
- Publish information to the directory
- Write/use an application that adds data to the directory
- Use an e-business software product that stores data in a directory

Benefits of a Directory

Directories:

- can store a large variety of data
  - Basic data types are string, integer, boolean, and binary (ex. JPEG photos)
  - Binary data can range from a few bytes to megabytes in size
  - Data can be a pointer to where an object is located (ex. CORBA)
- provide central data management
  - Consolidate duplicate information
- are available across an enterprise
  - Multiple applications, clients, and locations
- use an industry defined interface
  - Clients and servers can be on many platforms (platform independent)
- provide a standardized identity and authentication mechanism

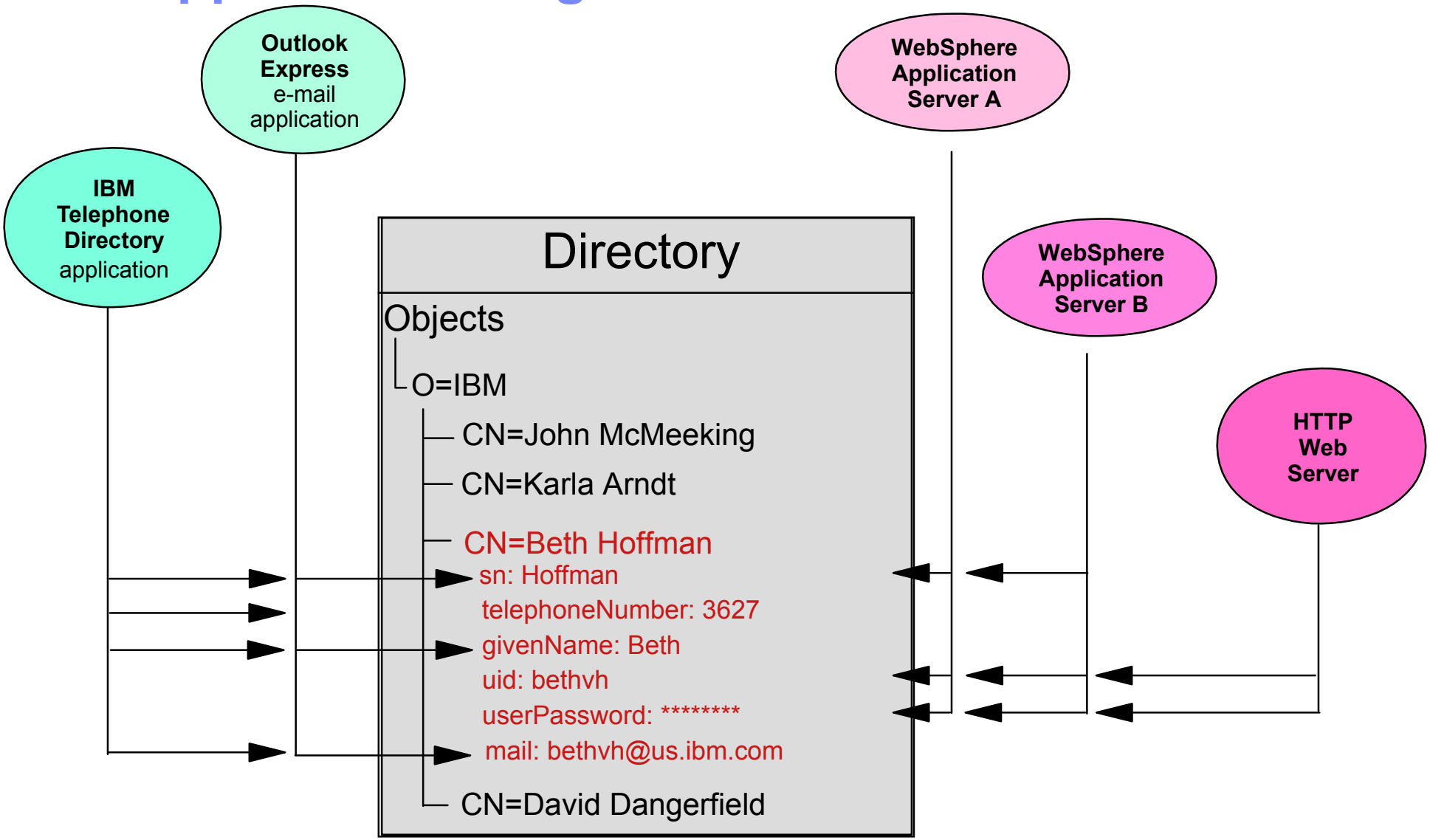
Benefits of a Directory (cont.)

Directories:

- support more granular access control
  - To a data entry or attribute level
- are fast
  - Store relatively static data used across your enterprise (ex. employee information, system information)
  - Tuned for read/search operations
- can work as a team (across many servers)
  - Referrals are hidden from the user or application
- allow data to be highly available
  - Data replication is supported

Uses of a Directory

Multi-Application Usage

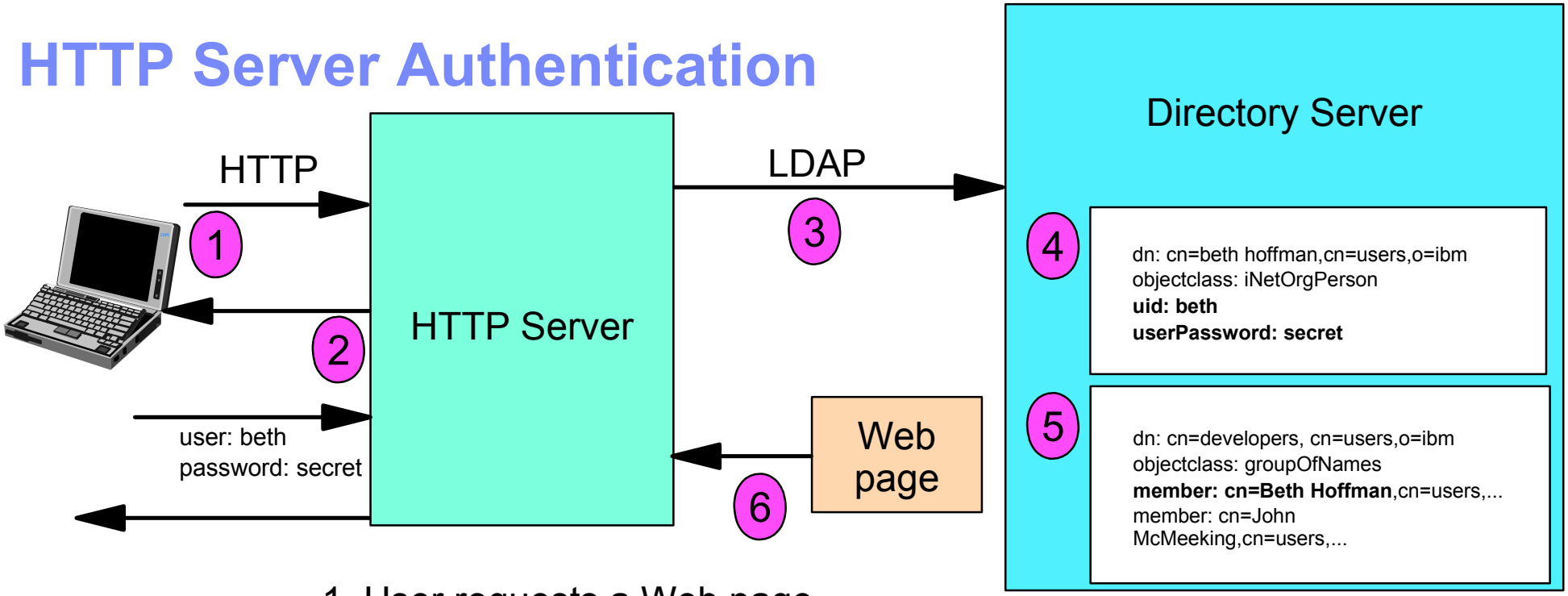


Common Uses: Middleware and Applications

- **User authentication**: **HTTP, WebSphere App, WebSphere Portal**
  - Share user authentication info (username, pwd, dig cert, client info) for accessing Web pages, Java applications, and portlets
- **Single sign-on/identity management**: **EIM**
  - Retrieve password everytime you use an app
  - Store identity mapping information
- **Enterprise phone book**: **ITD, Outlook Express, Domino**
  - Lookup people information
  - Secondary directory assistance
- **Centralize configuration**: **TCP QOS Policy, HTTP server config**
  - Share config across systems, servers
- **Locate system resources**: **Windows Add Printer wizard**
  - Lookup available printers at a location
  - Track system inventory

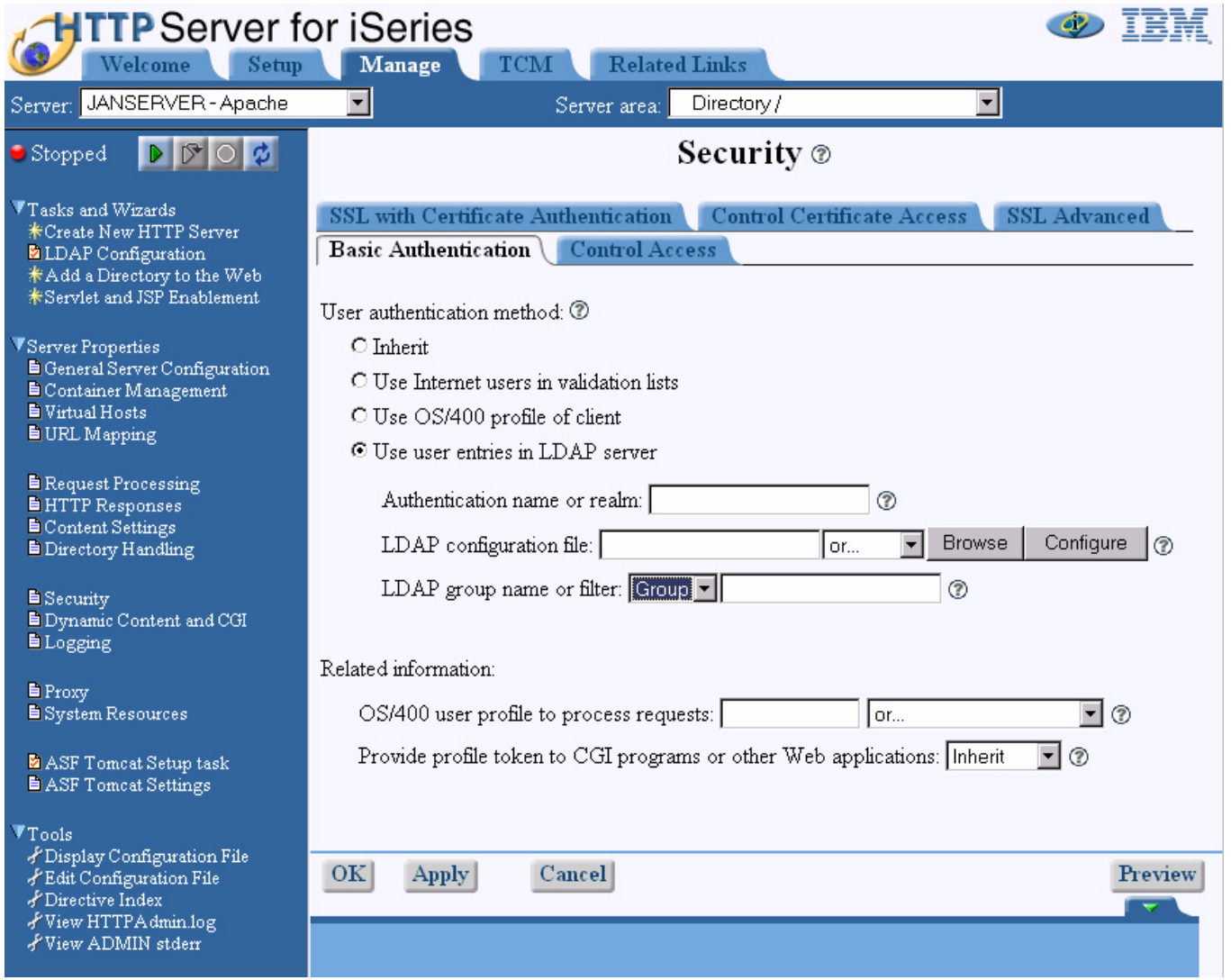
User Authentication

HTTP Server Authentication



1. User requests a Web page.
2. Web server prompts for user/pwd.
3. Web server asks Directory to search for user.
4. Passwords are compared.
5. Web server asks Directory if user is a member of the group.
6. Web server returns the Web page to the user.

IBM HTTP Server for iSeries (powered by Apache)

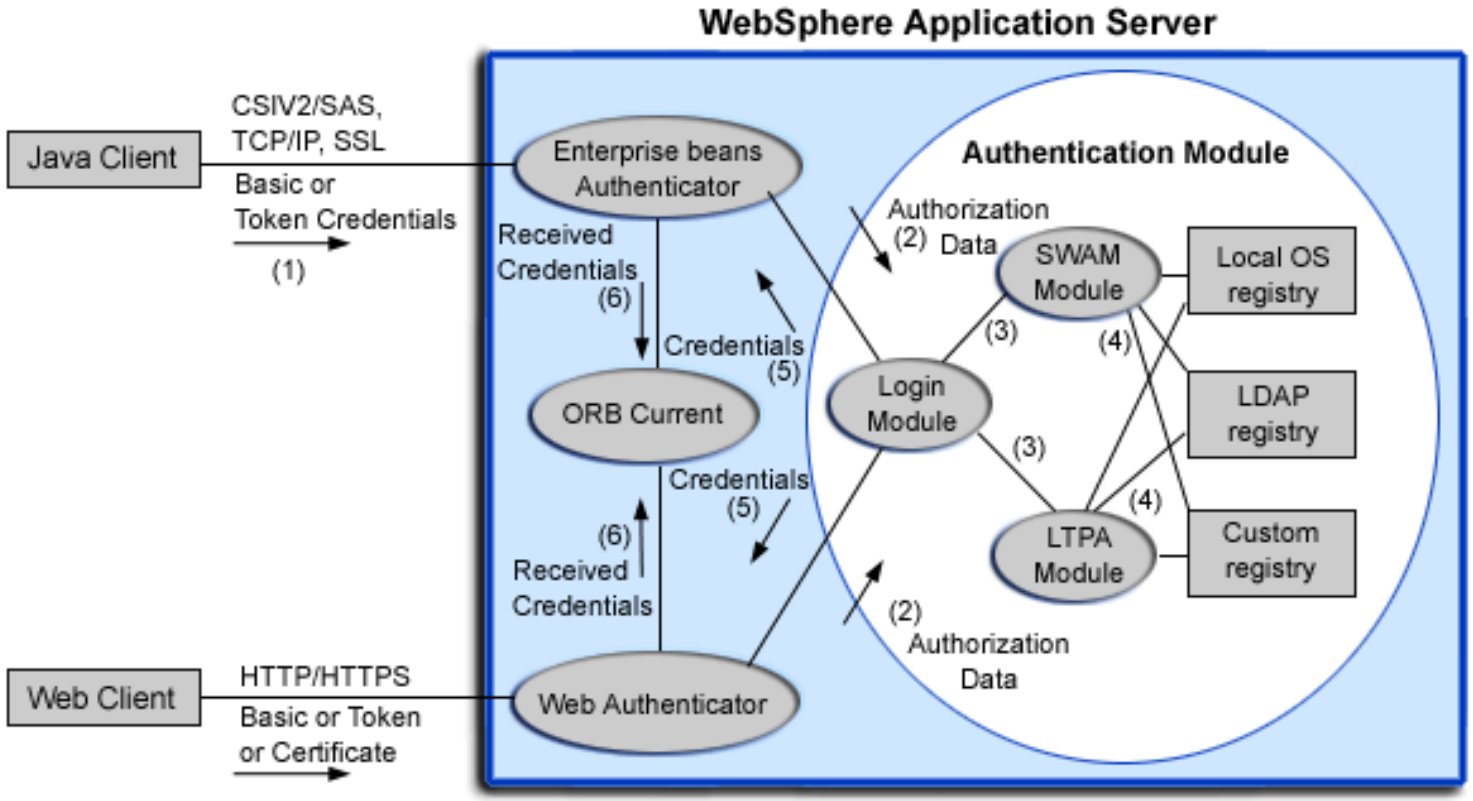


WebSphere Application Server v5.0 - Authentication

- The WebSphere Application Server provides two authentication mechanisms:
  1. Simple WebSphere Authentication Mechanism (SWAM)
  2. Lightweight Third Party Authentication (LTPA)
- For a WebSphere administrative domain (i.e. the set of servers, applications)
  - Only one authentication mechanism (LTPA or SWAM) can be configured
  - Only one user registry type (LocalOS, **LDAP**, or Custom) can be configured

- **When LDAP is chosen, the client information used for authenticating is stored in a directory.**
- **The use of Secure Sockets Layer (SSL) is supported between the WebSphere server and the LDAP server.**

WebSphere Authentication Process



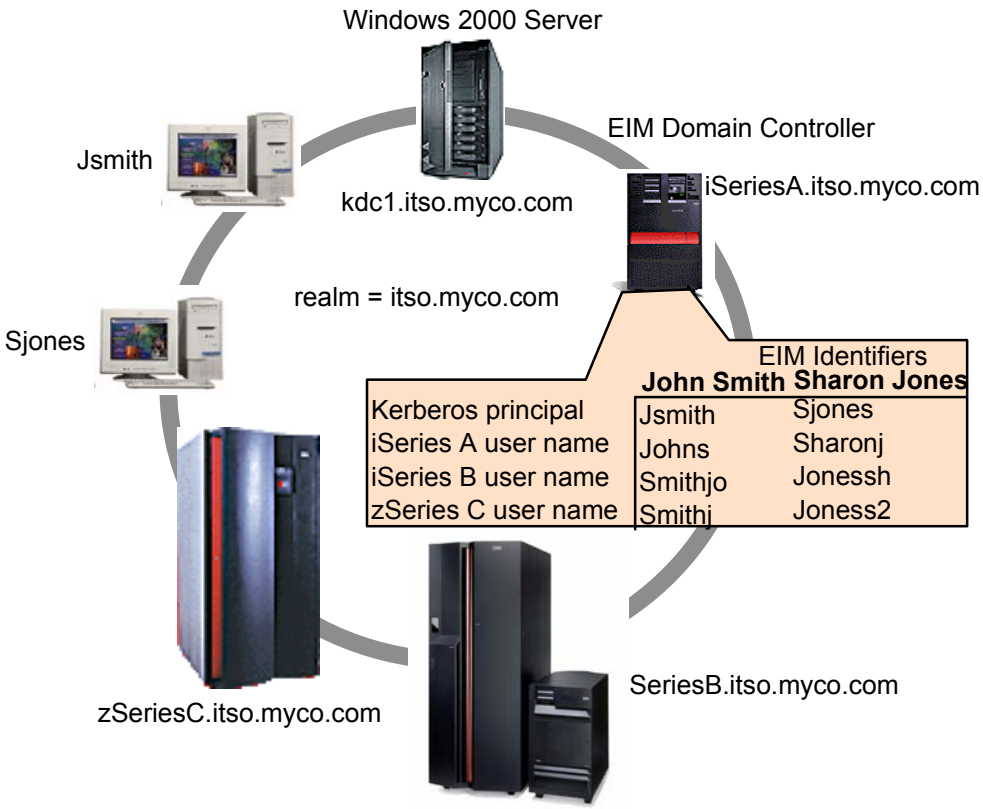
WebSphere Authentication Process - Details

1. **Authentication is required for enterprise beans clients (ex. servlets) and Web clients to access protected resources. The CSIV2, SAS, or HTTP protocol is used to the authentication info. The authentication info can be either basic (user ID and password), credential token (in case of LTPA), or client certificate. The Web authentication is performed by the Web authentication module and the enterprise bean is authenticated by the enterprise bean authentication module.**
2. **The Authentication module is implemented using Java Authentication and Authorization Service (JAAS) login module. The Web authenticator and enterprise bean authenticator pass the authentication data to the login module.**
3. **The login module can use either Lightweight Third Party Authentication (LTPA) or Simple WebSphere Authentication Mechanism (SWAM) for authentication.**
4. **The authentication module uses the user registry that is configured on the system to perform the authentication. There are three types of registries supported: one type is LDAP.**
5. **The login module creates and stores credential info. The credential is returned to the authenticator.**
6. **The authenticator stores the credentials in the ORB that is current for the authorization service and uses it to perform further access-control checking.**

Single Sign-On with EIM

What Is EIM?

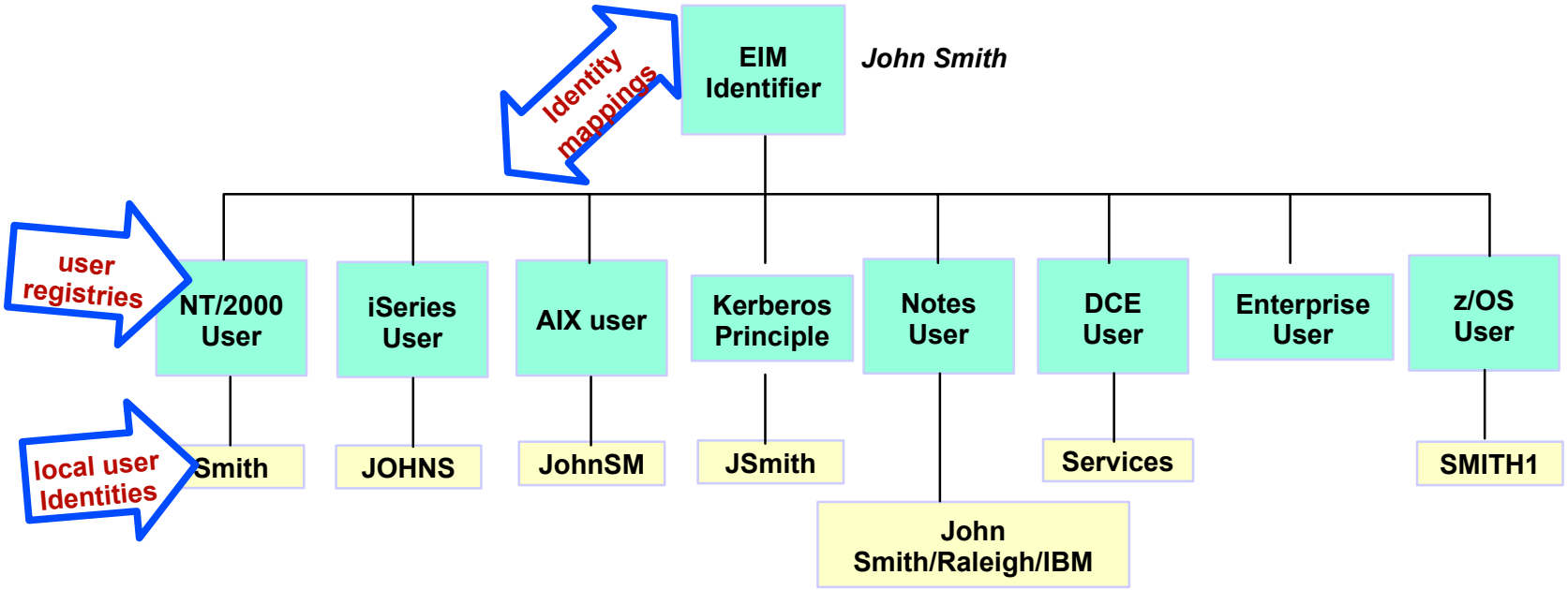
- Enterprise Identity Mapping (EIM) is a mechanism for **mapping** (associating) a person to the appropriate user identities in various registries throughout the enterprise.
- EIM enables single sign-on.



EIM Identifier and Mappings

An EIM identifier represents an actual person or entity in EIM

The identity associations (mappings) are stored in a well-known location, such as LDAP, with common services across platforms to access the mappings

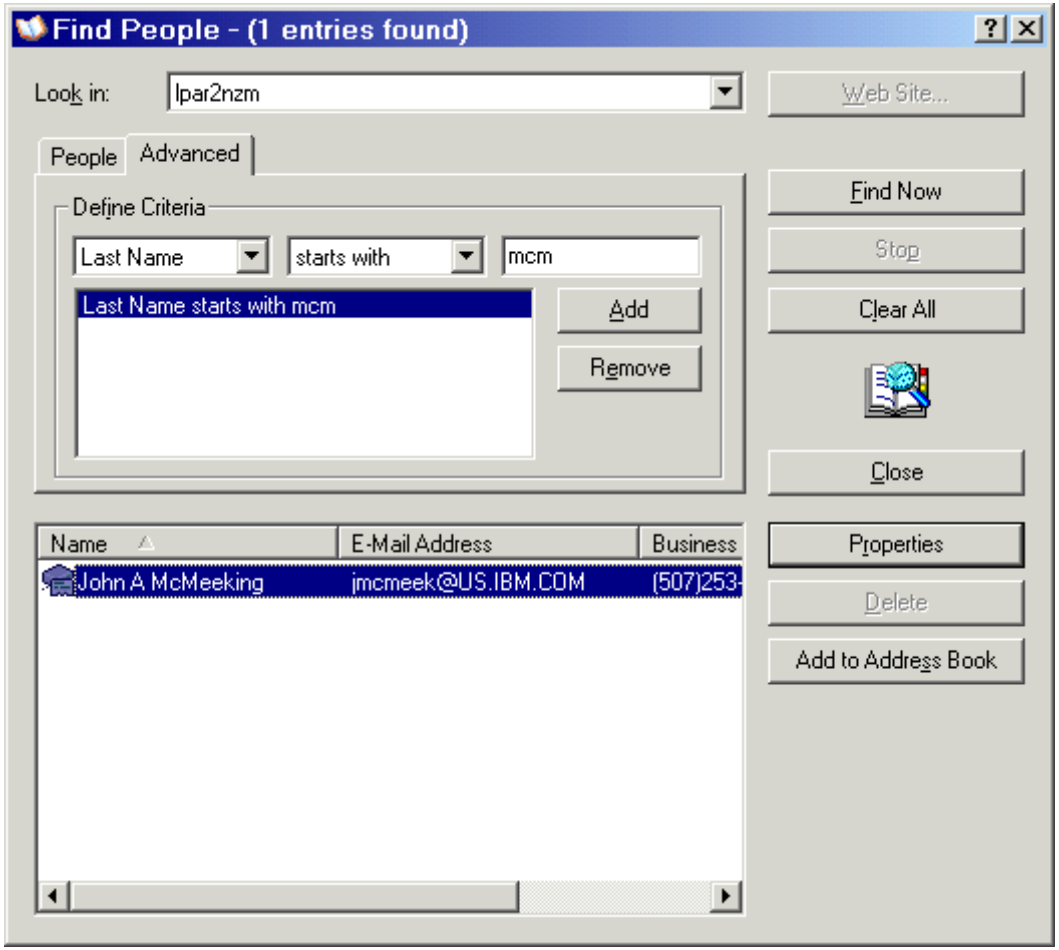


Application Use of Directory

e-mail Client Applications

- Use a shared Directory as their address book
- Most e-mail client applications in the market are LDAP-enabled
  - Domino/Lotus Notes
  - Netscape Messenger
  - Microsoft Outlook
- Each client identifies the LDAP server containing the user information
  - Multiple directories can be specified
  - Select the directory when searching for people

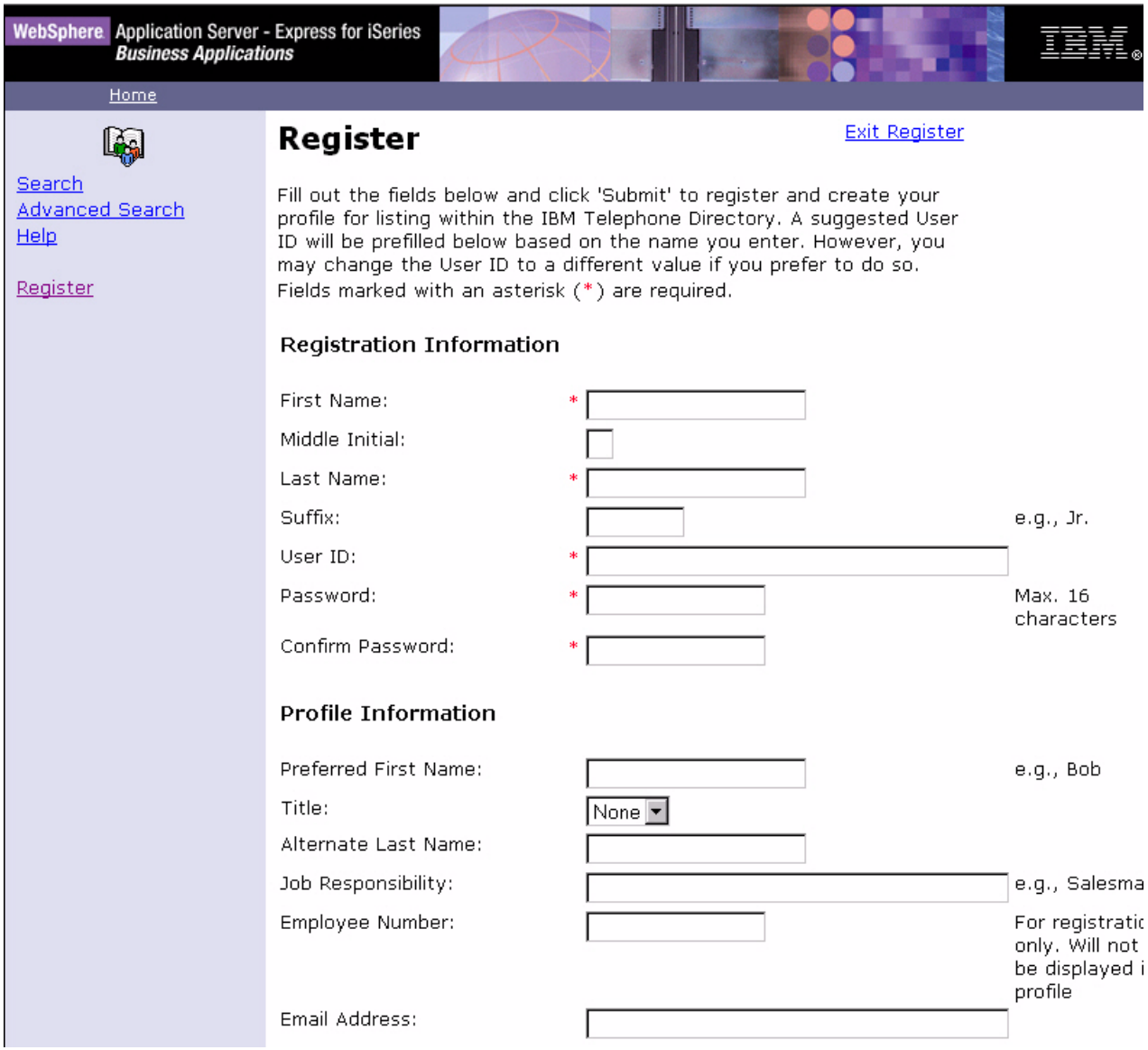
Find People - Outlook Express Example



IBM Telephone Directory

- Used with WebSphere Application Server - Express v5.0
- Business application
- Uses a Directory on iSeries to store people data
- No sample data is provided
- Publish SDD user data into the directory
- Or use the application to enter users

IBM Telephone Directory



Publishing

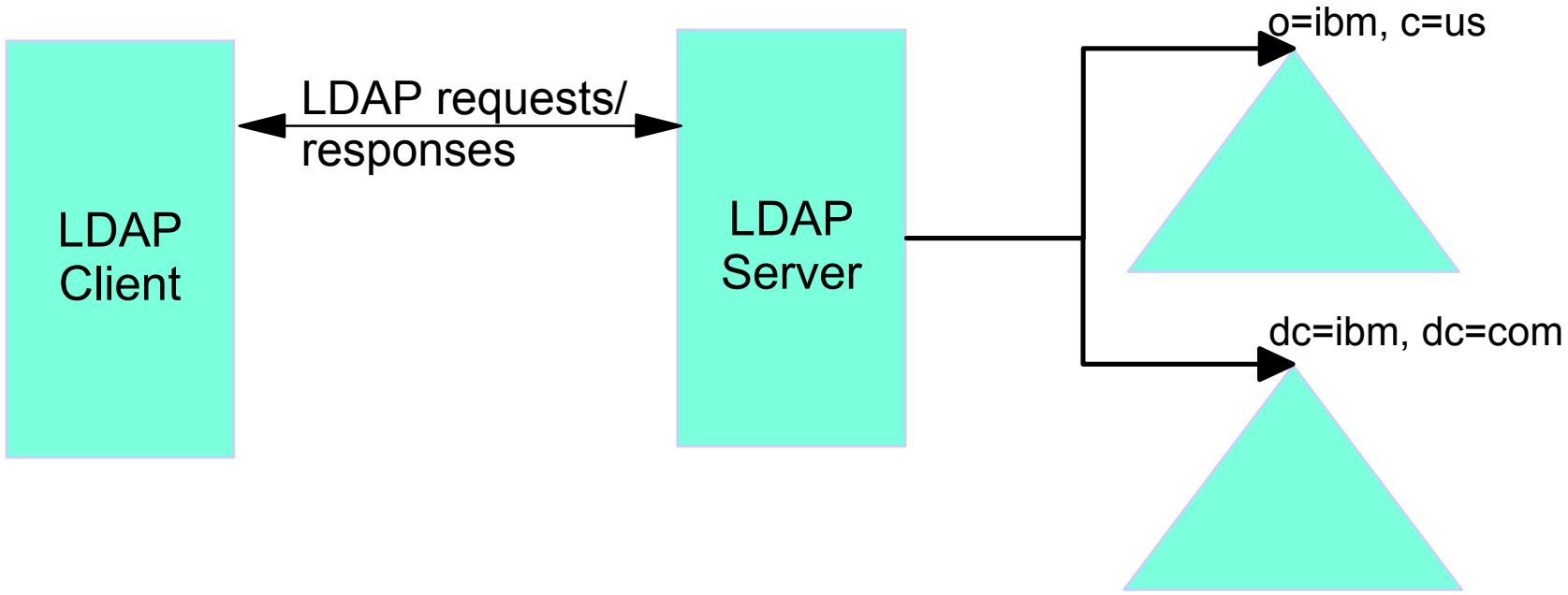
Four types of iSeries data can be published into a directory

1. **Users**
   - System Distribution Directory entries
2. **System Information**
   - Basic OS/400 system info
   - OS/400 printer hardware device descriptions
   - Management Central stores detailed system inventory information
3. **Printer Shares**
   - Publish printer shares to Active Directory
   - Use Add Printer wizard on Windows client to find print queues matching a certain criteria
4. **TCP/IP Quality of Service**
   - Define QOS policy information on one system
   - Other systems that need the same QOS config info can retrieve it using LDAP

Directory Concepts

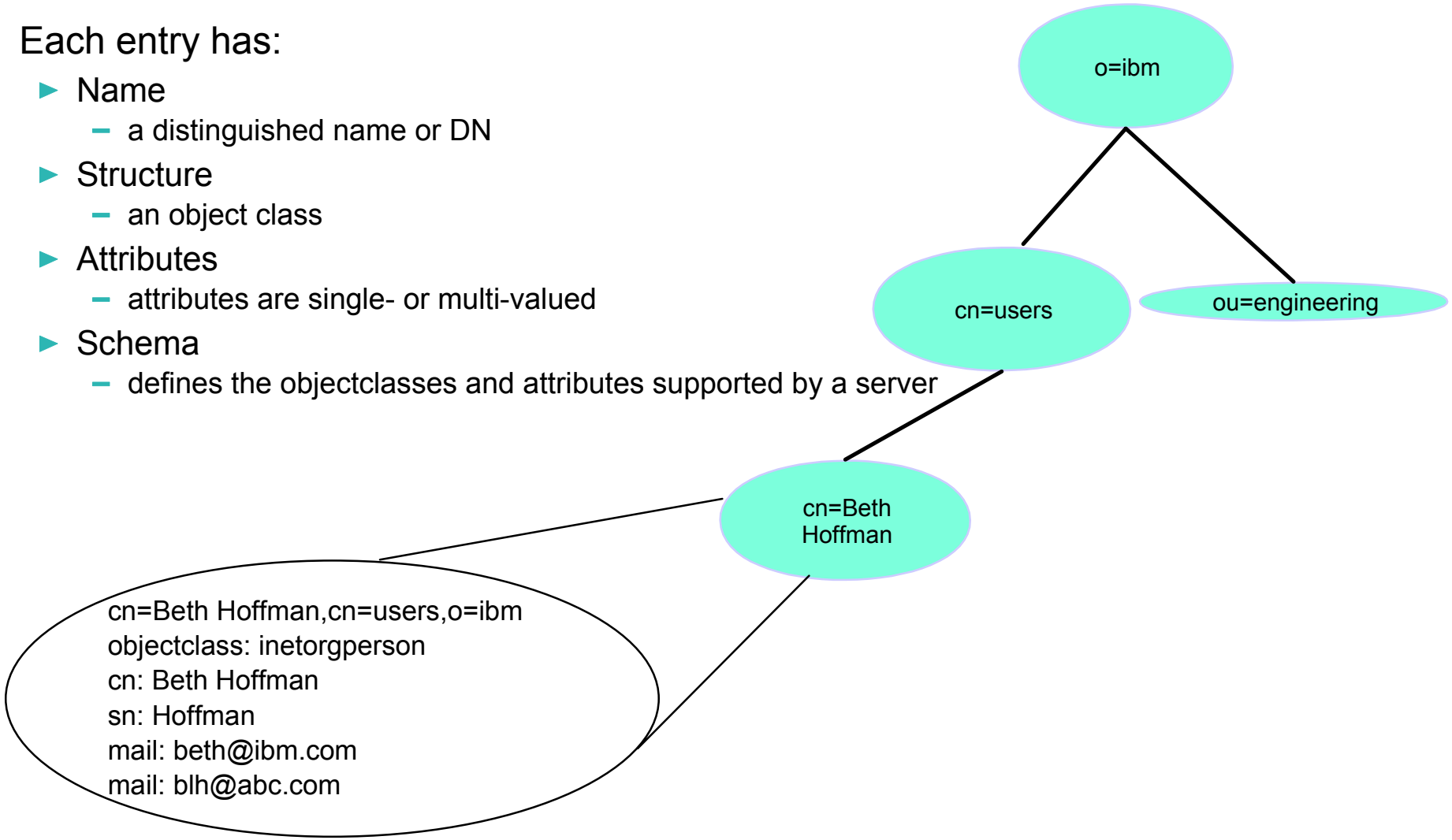
Directory Servers

- A Directory Server
  - Also called an LDAP server
  - Accepts and responds to directory requests
  - Manages a portion of a directory "namespace"



Directory Entries

- Each entry has:
  - Name
    - a distinguished name or DN
  - Structure
    - an object class
  - Attributes
    - attributes are single- or multi-valued
  - Schema
    - defines the objectclasses and attributes supported by a server



Directory Object Classes

- An entry's object class defines:
  - structure of an entry; unique identifier + name of object (person)
  - required attributes in an entry (common name, surname)
  - optional attributes in an entry (userPassword, telephoneNumber, description)
  - type of class (abstract, structural, or auxiliary)
- Each entry can be created from multiple object classes
  - The attributes are the UNION of those defined for each object class
  - Ex. person class + organizationalPerson

Directory Attributes

- Attributes are defined by their name, syntax, and matching rules
  - Syntax refers to the type of data stored in attribute values
    - Examples: String, Binary (i.e., JPEG photo), Integer, Boolean
  - Matching Rules define how equality and ordering comparisons are performed on attribute values
    - Examples: caseIgnoreMatch, caseExactMatch
- Attributes within an entry may be more "sensitive" than others
  - Example: cn (common name) vs. uid vs. userPassword
- Each attribute is assigned an access class (normal, sensitive, critical)
  - Defines high-level access on IBM servers
  - Examples: Anybody can read "normal" attributes such as the "mail" attribute.
    Members of the administrators group can write to userPassword.

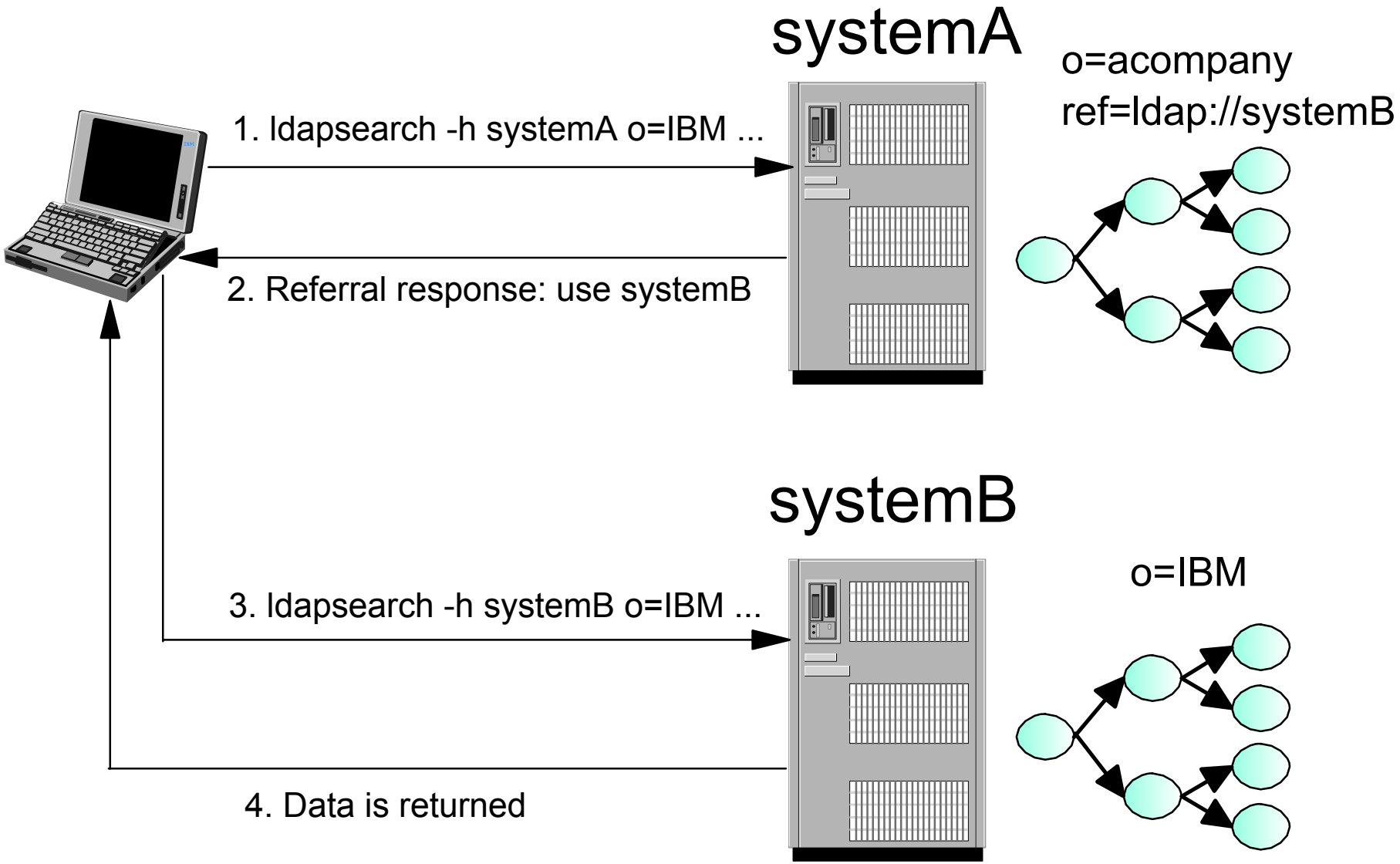
Directory Searches

- Search criteria
  - Starting point is base DN: o=acme
  - Search scope: object, one level or subtree
  - Filter: sn=Hoffman or more complex: objectclass=printer and location=...
- Supports two styles of queries
  - "whitepages" queries: retrieve an entry with a known name
  - "yellowpages" queries: look for entries matching specific criteria
- Filters support
  - AND/ORing components
  - existence of values, =, >=, <=, approximate, wildcards

Directory Referrals

- Allow LDAP servers to work in teams.
- If the DN that a client requests is not in one directory, the server can automatically send (refer) the request to any other LDAP server.
- The LDAP server sends referral info back to the client. It does not contact the other LDAP server.
- Referrals are "chased" by the client without the user knowing.
- Two types of referrals:
  - default referrals: the LDAP server refers clients whenever any DN is not in the directory.
  - DN-specific referrals: entries in the directory can be of the "referral" objectClass. This allows you to specify referrals that are based on what specific DN a client requests.

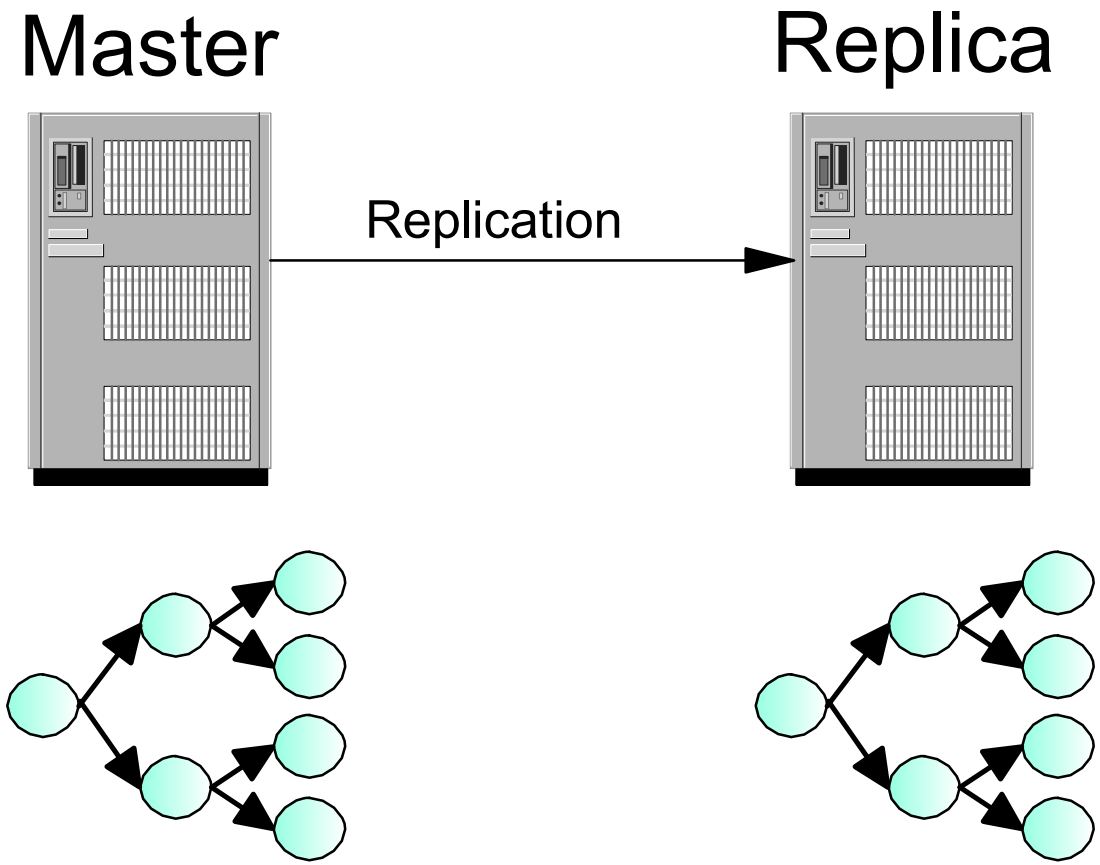
Directory Referral Example



Directory Replicas

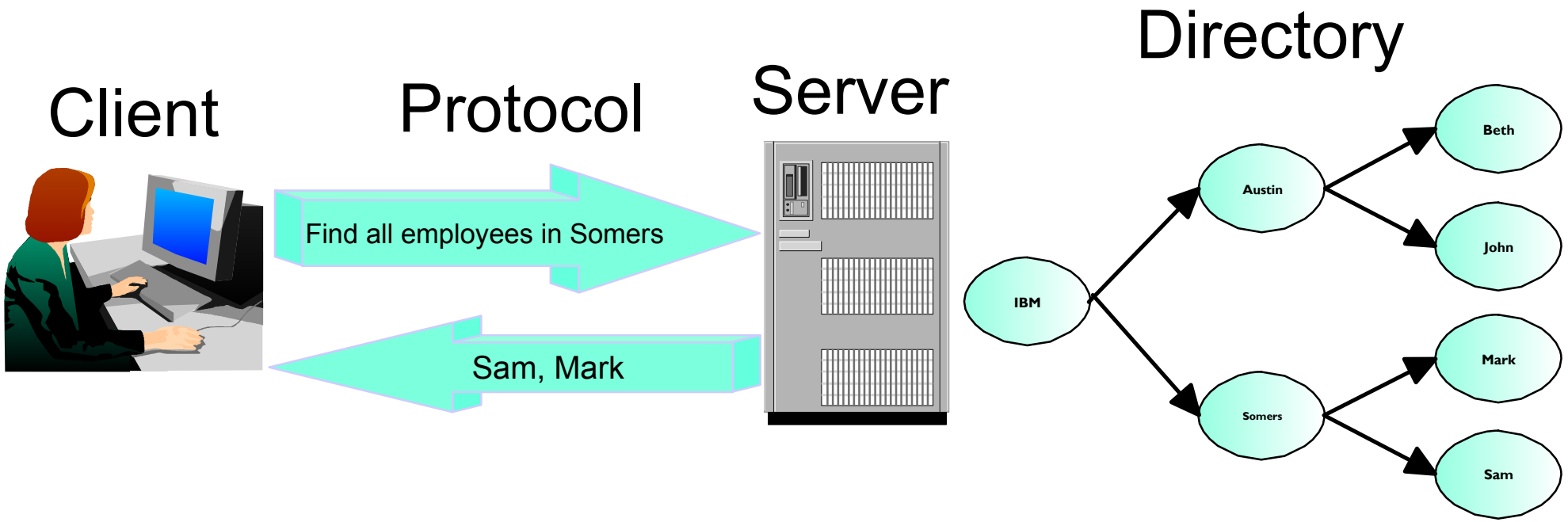
- An LDAP server can be a master server or a replica server.
- The data on a replica server is identical to the data on its master server.
- There are two key benefits for using replicas:
  - Replicas make directory searches faster. Instead of having all clients direct search requests to a single master server, you can split requests between the master server and the replica servers.
  - Replicas provide a backup to the master server. If the master server is unavailable, a replica can still fulfill search requests and provide access to directory data.
- Replica servers are read-only.
  - When an authorized user attempts to change an entry on a replica server, it refers the request to the master directory server.

Directory Replica Example



LDAP Overview

LDAP Example



LDAP Clients

1. LDAP client programming APIs
   - C/C++
   - Java through JNDI or Java LDAP (JDAP)
   - Directory Services Markup Language (DSML) can make LDAP a web service
2. Applications that use the APIs
   - mail clients, web servers, ...
3. Command-line tools to access/update the directory
   - ldapsearch, ldapmodify, ldapdelete, ...
4. General LDAP "browser" GUIs
   - IBM Directory Management Tool
   - LDAP Browser/Editor

LDAP Protocol

- LDAP - Lightweight Directory Access Protocol
- Standard Internet (TCP/IP based) protocol for accessing/updating directory information
- Protocol defines interfaces between a client and a server for requesting and returning information
- Version 3 defined in many RFCs
- New RFCs all the time (ex. LDIF format, Replication)

LDAP Servers

- Server vendors include:
  - Sun ONE Directory Server
  - Microsoft Active Directory
  - Novell e-Directory
  - IBM Directory Server (formerly SecureWay Directory)
- Integrated into many products:
  - Most e-mail clients: MS Exchange, MS Outlook, Netscape, Notes, ...
  - Public key infrastructure
  - Network components and more coming
- Virtual directory and meta-directory products also available

Overview of IBM Directory Server

IBM Directory Server

- Formerly IBM SecureWay Directory
- v4.1 made available in April 2002
- v5.1 made available in November 2002
- Server
  - DB2 backend
  - Web administration GUI
  - AIX 4.3.3+, Windows (NT, 2000), Linux (several), Solaris, HP-UX
  - SSL support
- Directory Client SDK
  - Command line utilities
  - C APIs
  - Directory Management Tool (Java directory content management GUI)
  - Also available for Windows 9x, XP

IBM Directory Server on iSeries

- Introduced in V4R3
  - Option 32 through V4R5
  - Included in base OS with V5R1
- IBM Directory Server
  - V5R2 is equivalent to IBM SecureWay Directory 3.2.2 + OS/400 features
  - LDAP V3 server (V2 prior to V4R5)
- Directory Client
  - ILE C APIs (callable from other ILE languages)
    - LDAP APIs, server config APIs
  - Java Naming and Directory Interfaces (JNDI)
  - QSHELL utilities (ldapsearch, ldapadd)
  - iSeries Navigator configuration/administration GUI
  - Publishing services
  - Directory Client SDK for Windows (includes DMT)
  - NLS Data support
    - the LDAP server can store data in any language by using UTF-8 w/ the protocol
- Schema
  - Base schema includes about 250 object classes and 1050 attribute types
  - Extensible schema (modify and add)

iSeries LDAP Server Features: Security

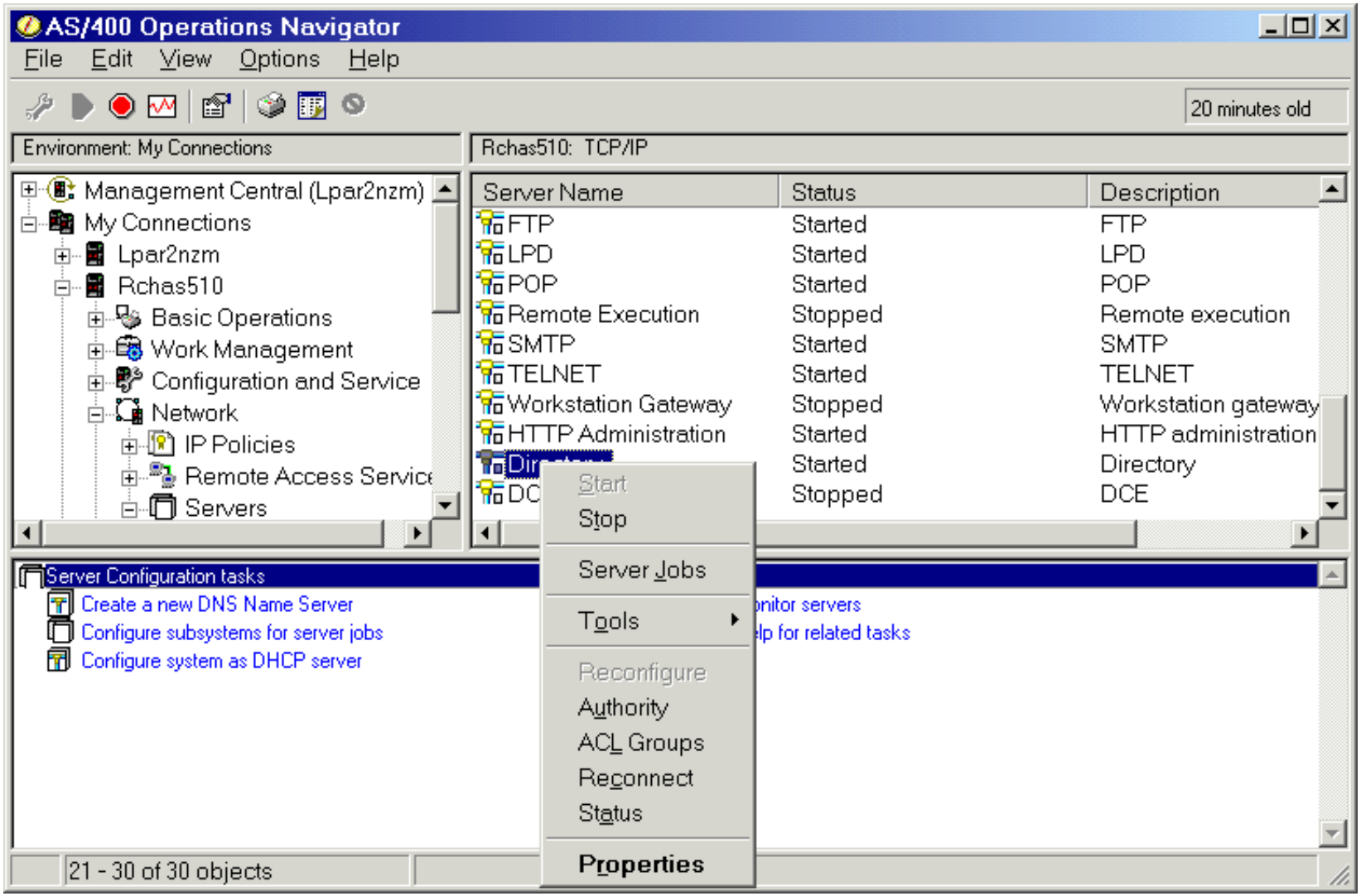
- Security Features:
  - Various authentication methods (DN/password, Kerberos, digital certificate)
  - Access control model
  - Secure connections using SSL and TLS
  - Clear text passwords are hashed and stored in validation lists
  - Encrypted passwords are stored in the directory entry
  - Server auditing integrated with operating system audit journal support
  - SQL tables are stored "securely"; can't use interactive SQL

New Features in V5R2

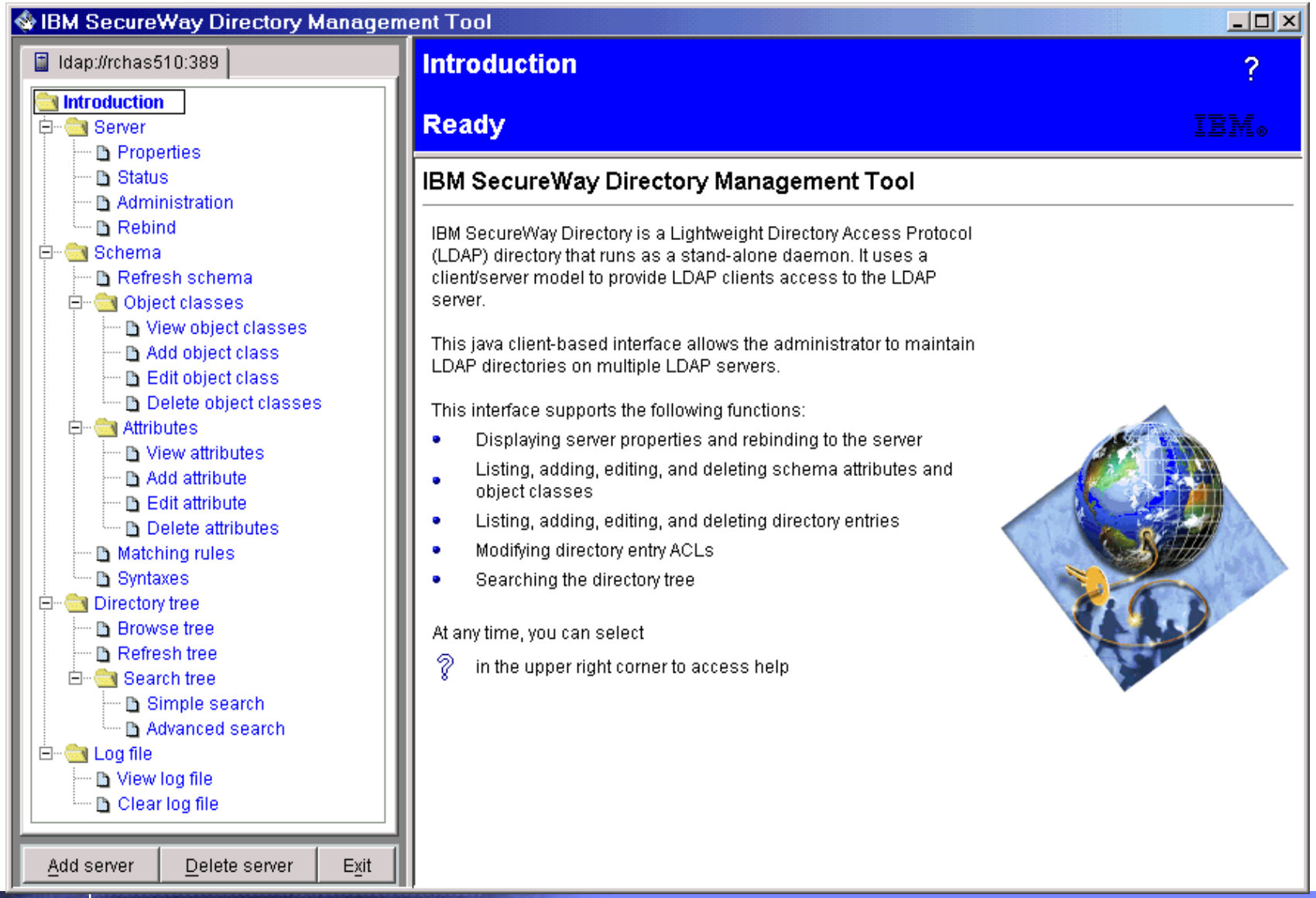
- Secure database backend.
- LDAP access to user profiles
  - create, modify, search, delete user profiles using standard LDAP operations
  - bind as a "projected" user (os400-profile=BETH,cn=accounts,...)
- Allow selected "projected" users to be LDAP administrators
- Specific IP address support (allows coexistence of many LDAP servers)
- Publishing QOS information

iSeries Configuration and Management Tools

iSeries Navigator



Directory Management Tool



Planning a New Directory

Planning a New Directory

- Design your directory content.
  - Decide the purpose and scope of the data.
  - Decide the names and types of the data entries.
  - Decide which data attributes are needed for each entry type.
  - Decide the source/input of the data.
- Organize your directory.
  - Design the schema (use existing, extend existing, create new).
  - Design the name space and hierarchy of your directory.
- Understand your security requirements.
- Design your server and network infrastructure.

Planning a New Directory: Security

- Decide whether access to some data needs to be controlled.
  - Access control lists (ACLs) can be used.
  - Determine if inherited access can be used.
- Decide what security measures you will use.
  - Choose how clients will authenticate with the server.
  - Decide whether secure transactions are required.
- Decide if you need OS/400 security auditing.

Planning a New Directory: Infrastructure

- Determine the number and location of LDAP servers.
  - Estimate availability and scalability needs.
  - Decide if replication or referrals are required.
- Determine how the data is distributed among them.
- Decide how large your directory will be.
  - Estimate how much storage you need. The size of the directory depends on:
    1. The number of attributes in the servers schema.
    2. The number of entries on the server.
    3. The type of information that you store on the server.
  - Example, an empty directory that uses the default Directory Services schema requires about 10 MB of storage. A directory with 1000 entries of typical employee information requires about 30 MB. This number will vary depending on the exact attributes that you use such as storing large objects such as pictures.

Summary

- You've learned:
  - What a directory is and the beneftis for an enterprise
  - The common uses of a directory
  - The applications that use it today
  - How LDAP works behind the scenes
  - IBM Directory Server product features
  - How to plan for a new directory
- What's next?
  - Learn how to use the tools to perform configuration
    - 420034: Configuring and Using the IBM Directory Server (LDAP)
  - Gain hands on experience now
    - 440178: OPEN LAB: IBM Directory Server (LDAP)
  - Back at the office
    - Design a simple directory, configure your LDAP server and create your first directory
  - Read advanced information

Next LDAP Presentation

- 420034: Configuring and Using the IBM Directory Server (LDAP)
  - Advanced LDAP concepts
    - LDAP terminology
    - Authentication methods
  - How to configure the server using the wizard
  - How to manage the server
  - Access control and groups
  - How to publish information to the server
  - Examples of entries and LDIF files
  - GUI tools for accessing and managing the server

LDAP Open Lab

- 430242: LAB: IBM Directory Server (LDAP)
  - Start and stop the server
  - Configure the server
  - Search entries in the directory
  - Create a suffix and add new directory entries
  - Work with directory data (delete/modify)
  - Import/export data using LDIF files
  - Use DMT
  - Work with the schema
  - Work with the change log
- 440144: LAB: Using LDAP Authentication with Apache
  - Create an HTTP server
  - Configure HTTP server to connect to LDAP server
  - Protect a web page using LDAP authentication

For More Information

- iSeries LDAP home page: www.ibm.com/eservers/iseries/ldap
- iSeries Information Center
  - Networking -> TCP/IP -> Directory Services (LDAP)
  - Programming -> CL and APIs -> APIs, look for Directory Services in APIs by category
- IBM Directory Server home page: www.ibm.com/software/network/directory/
- Redbooks (www.redbooks.ibm.com)
  - SG24-4986-00 Understanding LDAP
  - SG24-5110-00 LDAP Implementation Cookbook
  - SG24-6163-00 Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino
  - SG24-6193-00 Implementation and Practical Use of LDAP on IBM eServer iSeries
- "e-Directories Enterprise Software, Solutions, and Services". ISBN 0-201-70039-5. Published by Addison-Wesley Professional.

Appendix

- LDAP - Lightweight Directory Access Protocol
- RFC - Request for Comments
- LDIF - LDAP Data Interchange Format
- API - Application Programming Interface
- PKI - Public Key Infrastructure
- CRL - Certificate Revocation List
- EIM - Enterprise Identity Mapping
- SDD - System Distribution Directory
- QOS - Quality of Service

Trademarks and Disclaimers

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:
WebSphere WebSphere Application Server DB2 DB2/400 WebSphere Portal Server

AS/400	IBM
AS/400e	IBM (logo)
eServer	iSeries
	OS/400

Lotus®, Lotus Notes®, and Notes® are registered trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries, or both.
Domino is a trademark of Lotus Development Corporation and/or IBM Corporation.
MMX, Pentium, and ProShare are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.
Microsoft and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.
C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Other company, product or service names may be trademarks or service marks of others.

Information is provided "AS IS" without warranty of any kind.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information in this presentation concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Contact your local IBM office or IBM authorized reseller for the full text of the specific Statement of Direction.

Some information in this presentation addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Photographs shown are of engineering prototypes. Changes may be incorporated in production models.