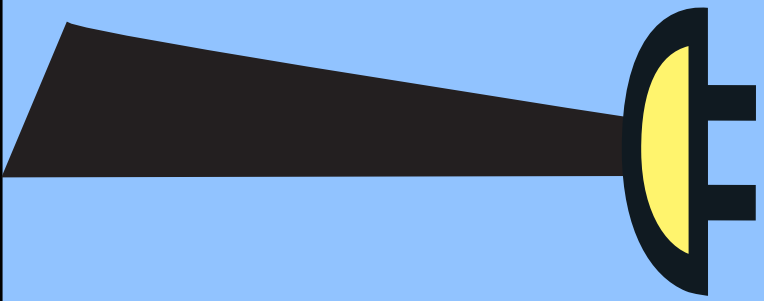
The promise of LDAP

Standards-based Internet Directories

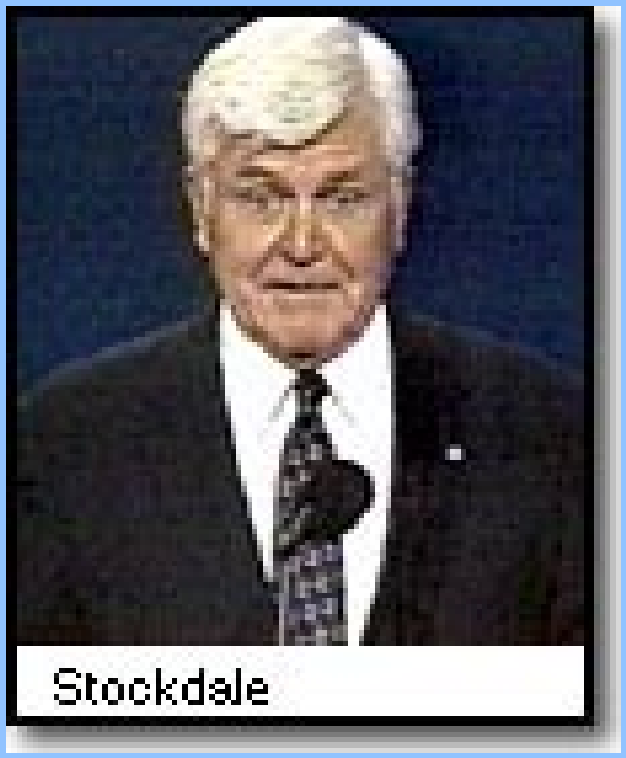
Paul A. Collins
One Click Systems



one click systems

Contents

Session goal #1—Hear from you



“Who am I?
Why am I here?”

—Adm. James Stockdale, presidential running mate and American hero

Session goal #2—Inform you

- What LDAP is
- What LDAP isn't, compared to other protocols and databases
- What you can do with it today and tomorrow
- Putting LDAP to work for you

Your role

- System Administrators / IT
- Developers
- Management
- End users

Your experience

- Know something about LDAP
- Have used LDAP
- Have set up server
- Want a solution!

What LDAP is

What LDAP is not

LDAP is…

- Lightweight Directory Access Protocol
- Born as front-end for X.500, the “heavy-weight” OSI directory
- Endorsed by 40 software companies as the Internet directory of choice in 1996
- 1998: Commercial LDAPv3 software

A Directory is…

- Fast access
- Many reads, few writes
- Standards-based interoperability
- Benefits

An LDAP Directory is not...

- Transactional database
- Relational database
- File or web server
- DNS (but will be part of SLP)

But what is LDAP?

- Lightweight Directory Access Protocol (RFC 2251, others)
- Standard for email lookups in email clients
- Operations: Search, filters, updates, bind (security)
- Standard schemas

Personal Data

- Contact info: Name/title/address/phone, sound, picture
- System info: Preferences, login & password, IP address

Service Data

- Device info: servers, printers, etc.
- Permissions and capabilities, perhaps

What you can do with LDAP

Today—Tomorrow

What you can do today

- Master address book
- Location moving—Netscape

What you can do today (cont.)

- Self-updating personal address books
- Public directories
- Organization directory

Server Products

- Active Directory (Microsoft)
- ClickMail Central Directory (OCS)
- Netscape Directory Server
- Oblix Corporate Service Center
- QuickMail Pro Directory System (CE)
- SLAPD (Univ. of Michigan)

Tomorrow

- Server authentication - single sign-on
- More application support
- Centralized application configuration (Mission Control)
- Resource allocation - implementing your policies
- Mail server support - groups!

Tomorrow (cont.)

- Worldwide directory webs
- Info publishing = user lookups.
  Systems support = authentication, configuration.
- E-commerce
- Interoperability improvements
- Self-updating interest-groups

LDAP on Macintosh

- Servers
- Mail Clients
- Netscape Client API for Mac (v2)
- Plug-in for Network Services Location (NSL)?
- Future Apple support

LDAP Case Study

Jeff Hodges

Kings Mountain Systems

Putting LDAP to work for you

How it's built

Planning your LDAP service

How it's built

- Information model
- Naming model
- Functional model
- Security model

Information model

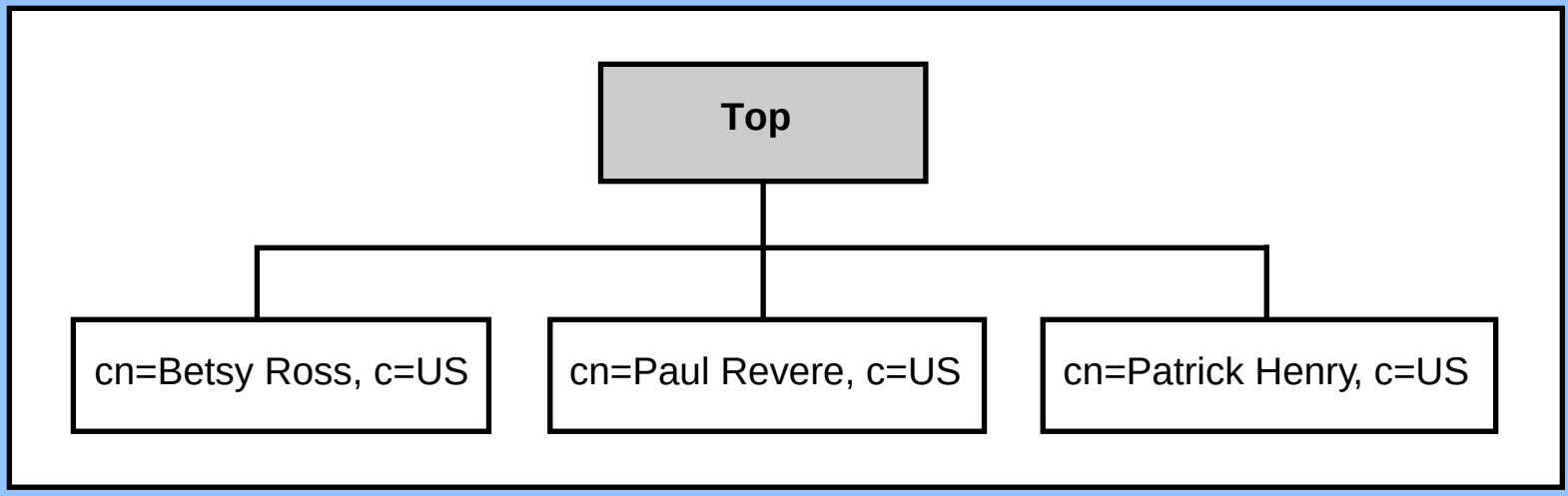
- Object classes
  - Person (name, phone, description)
  - OrgPerson (+ title, telex, ISDN)
  - InetOrgPerson (+ email, street, pager)
  - customPerson (+ your own attributes)
  - OrganizationalUnit = department…
  - Device (name, labeledURI)

Information model (cont.)

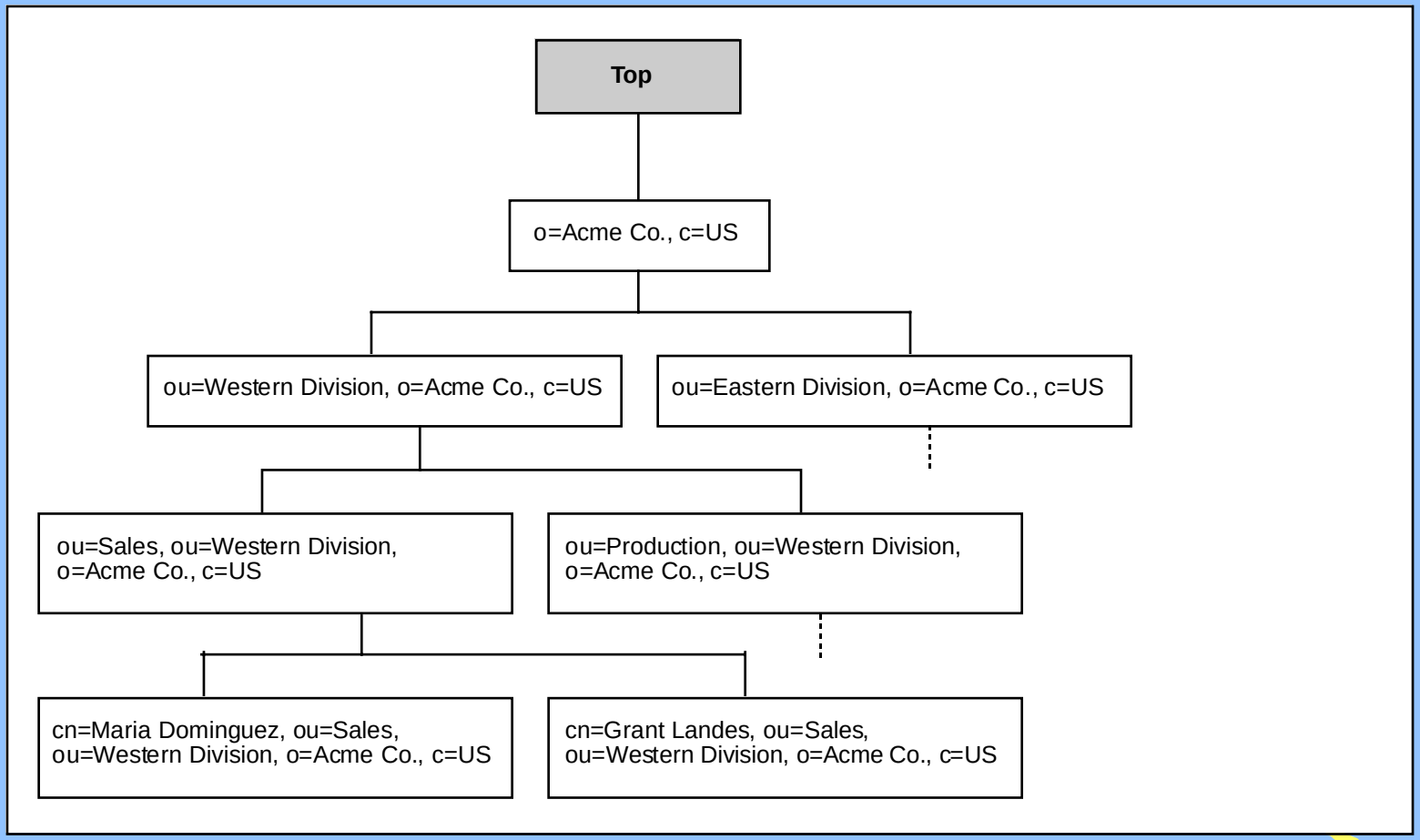
- Entries of various classes
- Schemas—what must/may be stored in each class
- Syntax and matching rules

Naming model

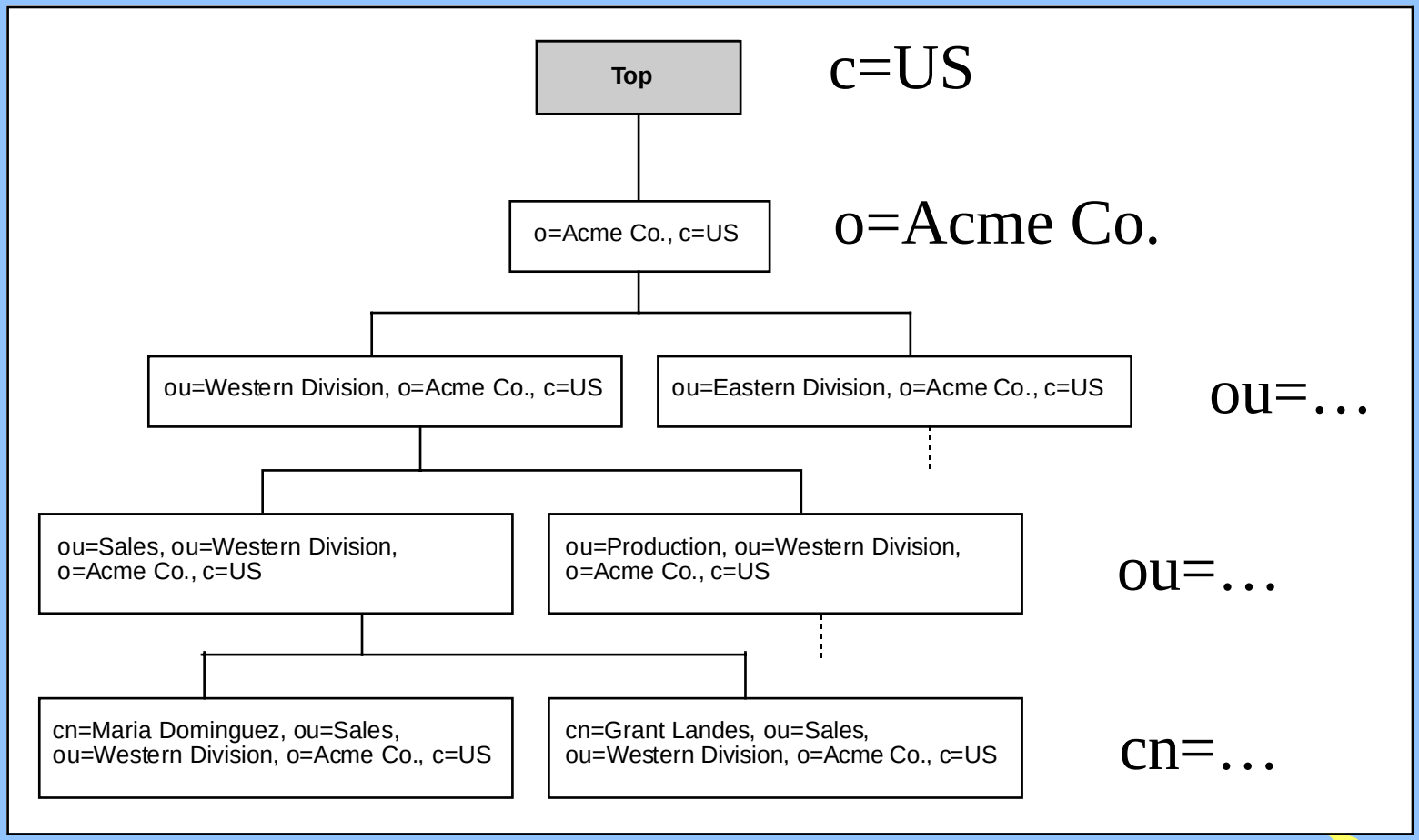
- Directory structure: flat



- Directory structure: tree (heirarchical)



Distinguished Name parts



Naming model (cont.)

- Distinguished Names (DN)
  - cn=Will Shakespeare, c=UK
  - uid=msmith, dc=netscape, dc=com
  - ssnhash=X8Sd9a8sd, o=Acme Co., c=US
- Geographic or domain naming
- Choose to fit your situation

Naming model (cont.)

- RDN and Naming Context
  - cn=Will Shakespeare, c=UK
  - uid=msmith, dc=netscape, dc=com
  - ssnhash=X8Sd9a8sd, o=Acme Co., c=US
- Multiple-hierarchy
- Global directory namespace

Functional model

- Internet protocol
- **Bind - Search**
- Others: Add, Delete, Modify, ModifyDN (move), Compare

Server	Client (LDAP-aware)
Bind:	
(waiting for TCP/IP call)	Hello, I'm "cn=Will Shakespeare, c=UK", my password is "bard".
Ok, Will, you're authorized.	
Search:	
	Starting at "c=UK", what people have "beth" in their common names? Just tell me their names and email addresses.

Server	Client
“cn=Beth Smith, c=UK” has common names “Beth Smith” and “Bethie Smith,” email address “beths@oneclick.com.”	
“cn=Angus Macbeth, c=UK” has common names “Angus Macbeth,” “Angus J. Macbeth,” and “Scotty Macbeth,” email is “macbeth@oneclick.com.”	
That’s all, 2 entries.	(next command or close TCP)

Security model

- Client bind (login), Self, by IP
- Read, Write
- Directory-wide
- Attributes
- Entries and branches

Done Jeff

Planning

Requirements

What do you want to provide?

- Contact info (can stop right here)
- Authentication
- Application preferences (Roaming)
- Policy implementation
- Networked resources: information, devices, applications

What Data?

- People: users, external contacts
- Things: servers, printers, user prefs
- Organizations: companies, divisions, departments, roles
- What attributes for each: email, phone, address, beverage
- Where is the data?

What Environment?

- Corporate, Internet environments
- Existing directories and data (legacy)
- Other LDAP servers (referrals)
- Resources: people, budgets, hardware.
- User interests and abilities
- Political realities

What Scale?

- How much data—number of entries
- How much speed—simultaneous users
- Replication can help

How much Security?

- Personal and organizational privacy
- Protection from attacks and failures
- How much do users see, create, and maintain?
- Who gets access to what? Public, In-house, Personal (self)

How much Reliability?

- Authoritative source(s)
- Can LDAP become the authoritative source?
- How is everything backed up?
- Replication can help, again.

Planning

Structure

Structure—Flat or tree?

- Flat: Easy, few hundred entries
- Tree: Flexible, browseable, application support
- Tree species: Organization chart, geography, domain/network.

Structure—What is stored?

- Schema - entries (objects) that have attributes
- Data types - text, binary, certificates, passwords

Structure—Naming system?

- Common names (“John Smith”)
- User IDs or serials
- Email addresses
- Combinations

Other databases and directories

- How is data shared/sync'ed?
- Will LDAP replace or coexist?
- Changes from outside the system?
- LDAP replication with other LDAP servers

Other directories—integration

- LDAP front-ends
- Proprietary servers' LDAP modules
- WebStar LDAP module
- QuickMail Office LDAP module
- AppleShare IP Users & Groups
- ClickMail mirror of AppleShare IP

Planning

Methods

How is data created/updated?

- Import LDIF
- Import tab-delimited
- Local edit, in server application
- Mirror AppleShare IP Users
- Enter in LDAP write client
- Web CGI entry

LDIF: LDAP Data Interchange Format

```
dn: cn=Wilma Flintstone, c=US
objectclass: emailPerson
objectclass: person
objectclass: top
cn: Wilma Flintstone
givenname: Wilma
homephone: +1 999 888 7111
mail: wima@bedrock.com
seealso: cn=Fred Flintstone, c=US
sn: Flintstone
telephonenumber: +1 999 787 9000
createTimestamp: 19980410132537Z
modifiersName: cn=Directory Manager, c=US
```

Who owns/maintains data?

- Administrator
- Managers
- Users/self

Do users cache directory data?

- Search server each time
- Download/cache all or some data
- Replication-aware client software?

Planning

Software

Server and client software

- LDAP versions, extensions supported?
- Security features: SSL, IP address, ACL or equivalents
- Support for your planned requirements
- Interoperability

Server software

- Import/export formats, updating
- Replication through LDAP or AppleShare Registry, AppleEvents, etc.
- Local, remote administration

More Information

Final tips…

- Attribute syntaxes are not enforced
- Outlook search base—check client's Internet Config
- FileMaker template helps create schema-correct data

Internet RFCs

- LDAPv3, plus extensions - RFC 2251
- Attribute Syntax - RFC 2252
- String Representation of Distinguished Names—RFC 2253
- String Representation of Search Filters—RFC 2254
- Extensions

LDAP's core definitions

- ITU's X.500
- ObjectClasses, attributes
- http://www.itu.ch/publications/index.html

Where to go next

- Book: Understanding and Deploying LDAP Directory Services
- LDAP Roadmap & FAQ—
  http://www.kingsmountain.com/ldapRoadmap.shtml
- This talk & more—
  http://www.oneclick.com/info/macworld/

Summary

- What LDAP is and isn't
- What you can do with LDAP
- Putting LDAP to work for you:
- Requirements
- Structures
- Security
- Methods
- Software

Q & A

(Evaluation Forms)

The promise of LDAP

Standards-based Internet Directories

Thank you!

Paul A. Collins paul@oneclick.com
One Click Systems http://www.oneclick.com

one click systems