Tema 5: Directorio

Introducción

Historia

LDAP

X.500 vs LDAP

ACAP

Bibliografía

1. Introducción

- Directorio
  - Guía o lista de direcciones de determinada clase de personas, casas comerciales ... (María Moliner)
  - Listado de información con objetos (ordenados según un determinado criterio) y detalles de los mismos
  - Ejemplo: listín telefónico
  - Permiten encontrar recursos a usuarios y aplicaciones
  - Uso del directorio
    - Páginas blancas: nombre -> atributos
    - Páginas amarillas: búsqueda por atributos

1. Introducción

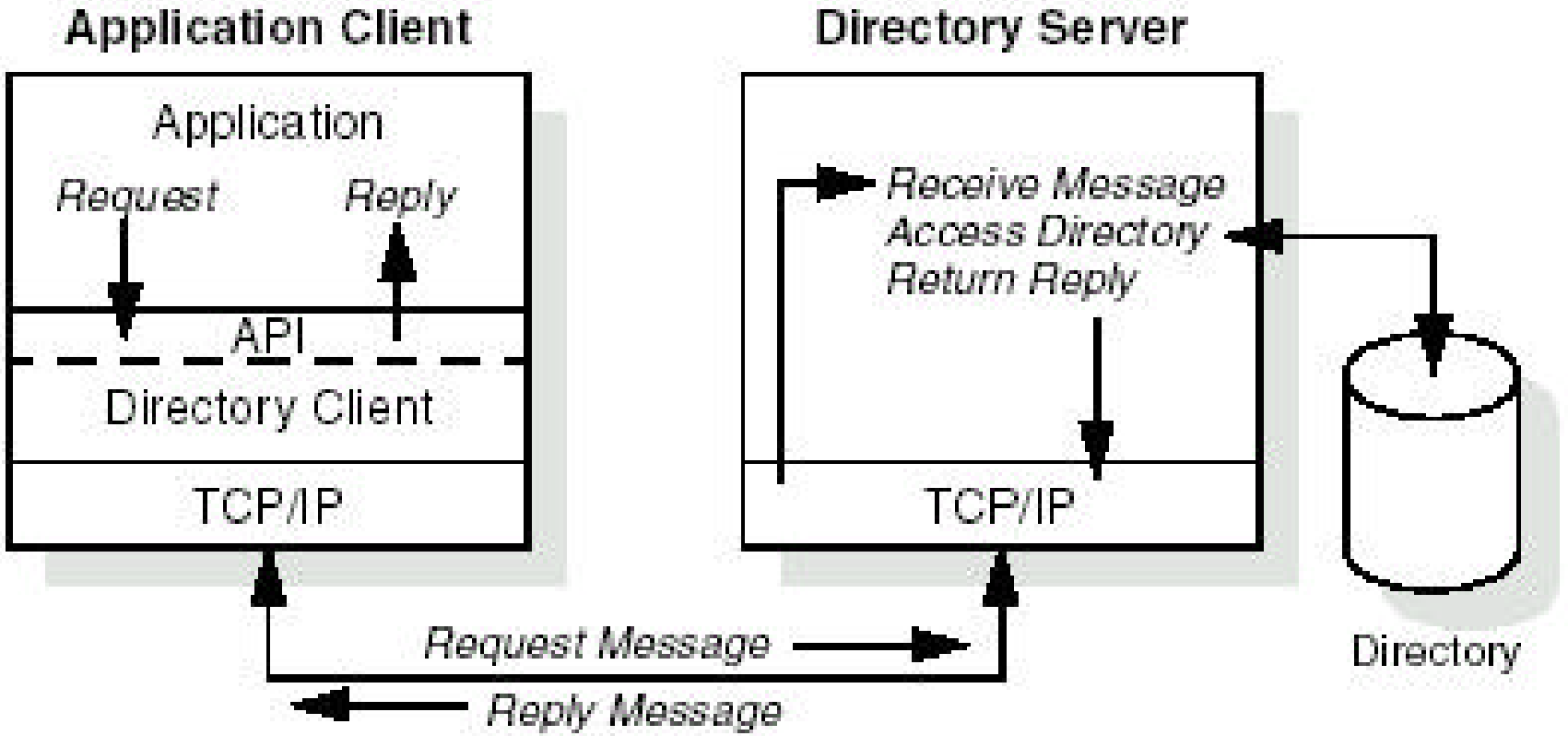
- Directorio informático
  - Base de datos especializada
  - Información de objetos
    - Descriptiva
    - Basada en atributos
  - Ejemplos:
    - Empleados: @, teléfono, fax, certificado criptográfico
    - Impresoras: ubicación, páginas/minuto, formatos soportados ...

1. Introducción

- Directorio vs Base de datos
  - Info. leída mucho más que escrita
  - Lecturas y búsquedas optimizadas
  - No apropiadas para almacenar info que cambia a menudo
  - No soporta transacciones (en general)
    - Inconsistencias temporales aceptables
  - Protocolo de acceso más sencillo
    - LDAP vs SQL
  - Base de datos sencilla y optimizada utilizada por aplicaciones pequeñas y sencillas

1. Introducción

- Clientes y servidores



1. Introducción

- Descripción servicio directorio
  - Según ámbito información:
    - Local: info. DIIS
    - Global: info unizar
  - Según topología directorio:
    - Centralizado: un servidor de directorio
    - Distribuido
      - Particionado
      - Replicado

1. Introducción

- Objetivo: directorio común
  - Independiente aplicaciones
    - Compartido por distintas aplicaciones
    - Evitar replicación de info en directorios específicos
  - Independiente plataforma
  - Funcionalidades de búsqueda, administración, particionado ...
  - Estándar abierto y público
  - API estándar
  - Robusto, seguro, escalable ...

... **LDAP**

1. Introducción

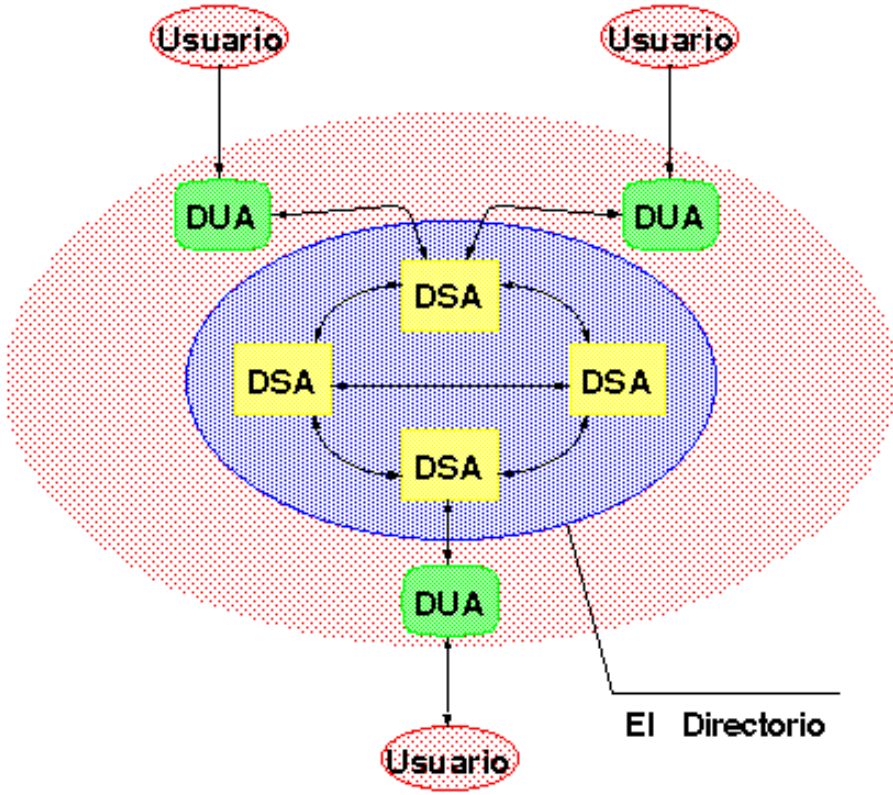
- Servicios de directorio
  - X.500: servicio de directorio OSI
  - LDAP: Lightweight Directory Access Protocol
  - Whois (DNS), Whois++
  - Netware Directory Service (NDS)

2. X.500

- CCITT
  - 1988: X500
  - 1990: ISO 9594, X500-X521
  - Extendido en 1993
- Servicio de directorio global OSI
- BD distribuida entre muchos servidores
  - Aparentemente centralizada
- Características
  - Jerarquía, cooperación, replicación, caches ...

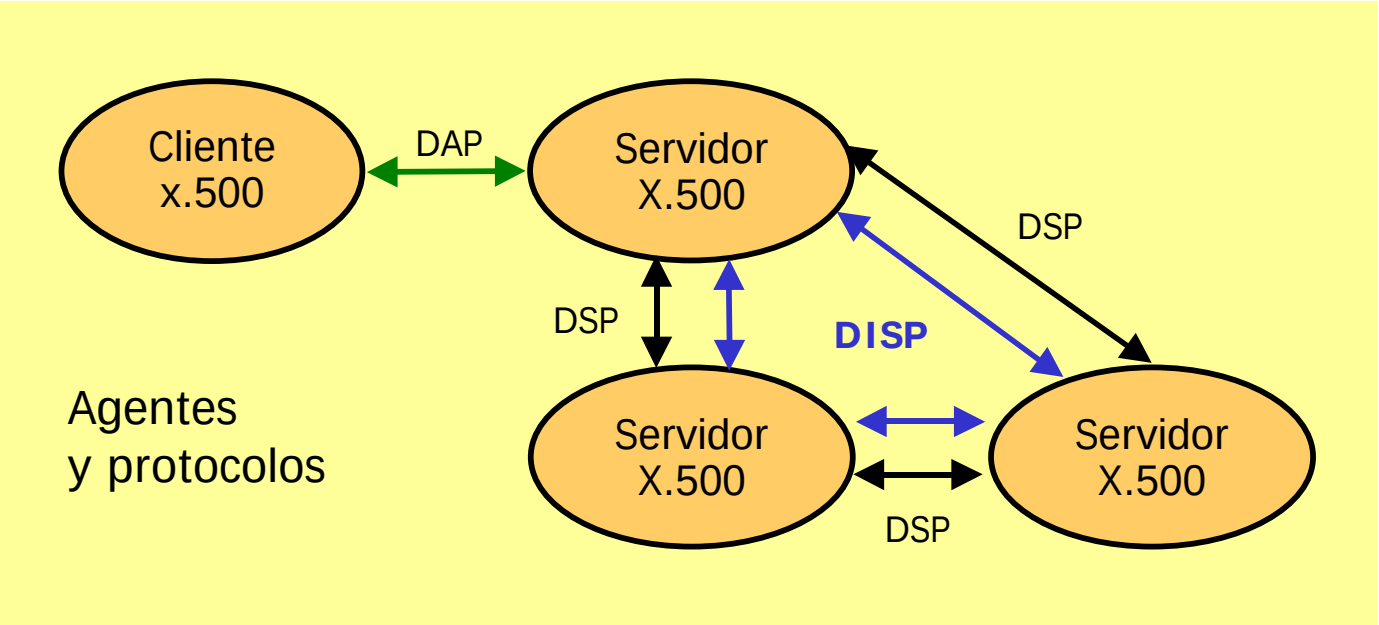
2. X.500. Agentes

- DIB - Base de Información del Directorio
  - Información contenida en el directorio
  - Objetos: personas, organizaciones, aplicaciones OSI ...
- DSAs – Agentes de Sistema del Directorio
  - Servidores
  - Mantienen la info distribuida del directorio (objetos)
  - BD local
- DUAs – Agentes de Usuarios del Directorio
  - Clientes



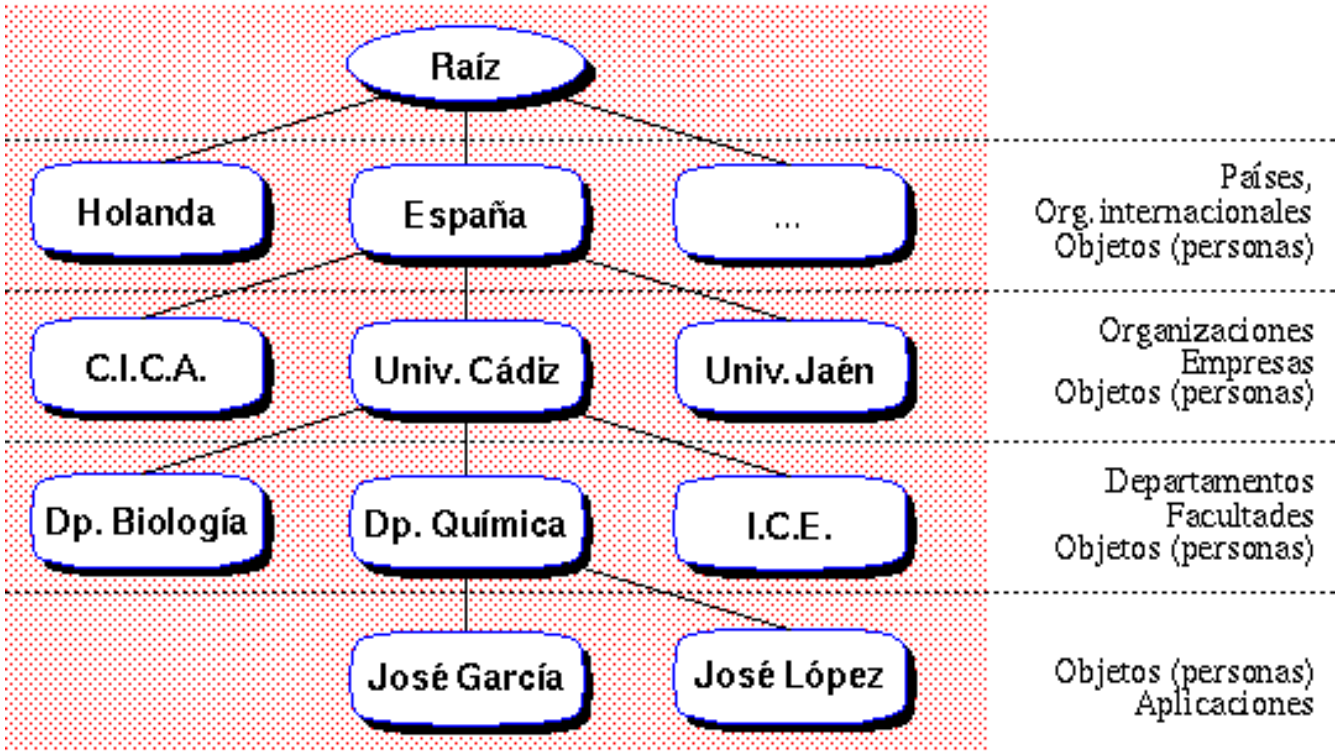
2. X.500

- Protocolos de X.500 (capa aplicaciòn)
  - DAP: Directory Access Protocol (capa superior pila OSI)
  - DSP: Directory System Protocol
  - DISP: Directory Information Shadowing Protocol



2. X.500

- Estructura del directorio
  - DIT: Árbol de Información del Directorio
    - Búsquedas rápidas y sencillas
  - Jerárquica en niveles (origen en raíz)
  - Un encargado de mantenimiento por nivel



2. X.500

- Entradas del directorio
  - DN: nombre único de cada objeto
    - Nombre distintivo formado por atributos
    - País (c), organización (o), unidad organización (ou), nombre del objeto (cn), ...
  - RDN: Nombres Distintivos Relativos
  - DN = Secuencia RDN (desde raíz)

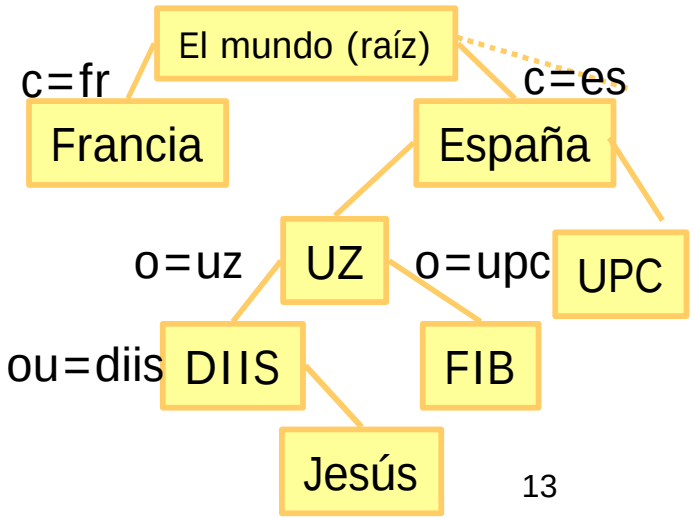
    DN: "@c=ES @o=Universidad de Zaragoza @ou= Dpto. Informática e Ingeniería de Sistemas @cn= Jesús Alastruey"

    RDN 1: c=ES

    RDN 2: o= Universidad de Zaragoza

    RDN 3: ou= Dpto. Informática e Ingeniería de Sistemas

    RDN 4: cn= Jesús Alastruey
  - Operaciones DUAs
    - Añadir, borrar, modificar entradas
    - Lectura, listado, búsqueda de objetos



2. X.500

- Aplicaciones suministradas por el directorio
  - Interpersonales: usuario-directorio
    - Páginas blancas
      - Búsqueda por DN y conjunto de atributos del objeto buscado
      - Ej: personal del departamento de Informática de la UZ
    - Páginas amarillas
      - Ej: personal del departamento de Informática de la UZ que se llame Lorenzo
  - Entre sistemas: aplicaciones OSI-directorio
    - Directorio selecciona aplicación que realiza servicio deseado
    - FTAM: transferencia, acceso y gestión de ficheros distribuidos

2. X.500

- Servicio de directorio OSI
  - Necesita la pila de protocolos OSI entera
  - Complejo
  - Los clientes son “pesados” (necesitan muchos recursos)

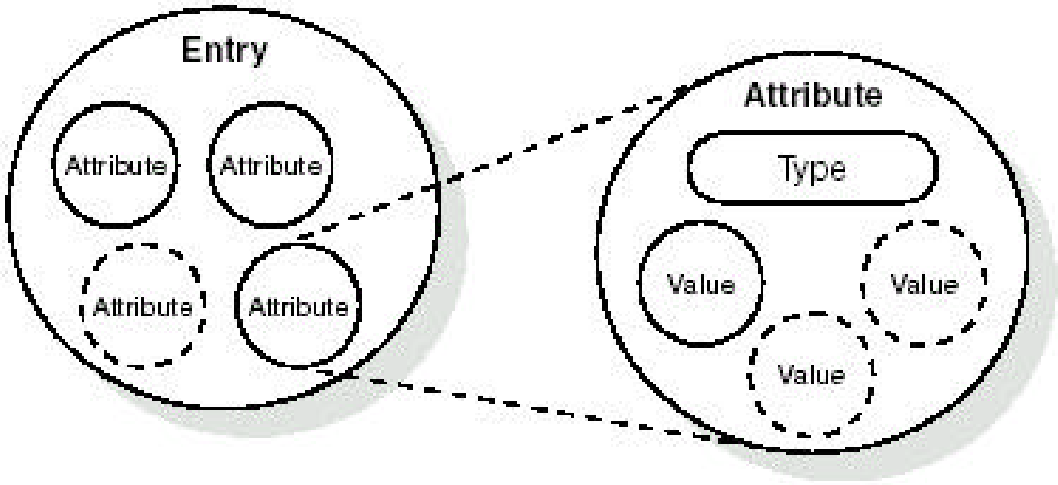
- RedIris
  - 1-Octubre-2001
    - Apagado del servidor de directorio basado en X.500 que mantenía la raíz de España
    - Nuevo Servicio de Directorio basado en servidores LDAP
  - http://www.rediris.es/ldap/novedades/2001/20011001.es.html

3. LDAP

- Lightweight Directory Access Protocol
  - LDAP: RFC 1777 (histórico)
  - LDAP v2: RFC 1777, 1778, 1779, 1959, 1960, 3494 (información)
  - LDAP v3: RFC 2251-2256, 2829, 2830, 3377 (propuesto)
- Transporte y formato de mensajes para acceso a directorios globales de información
  - Visión del directorio independiente del servidor
- Basado en DAP (X.500)
  - Más sencillo
  - Pila protocolos TCP/IP

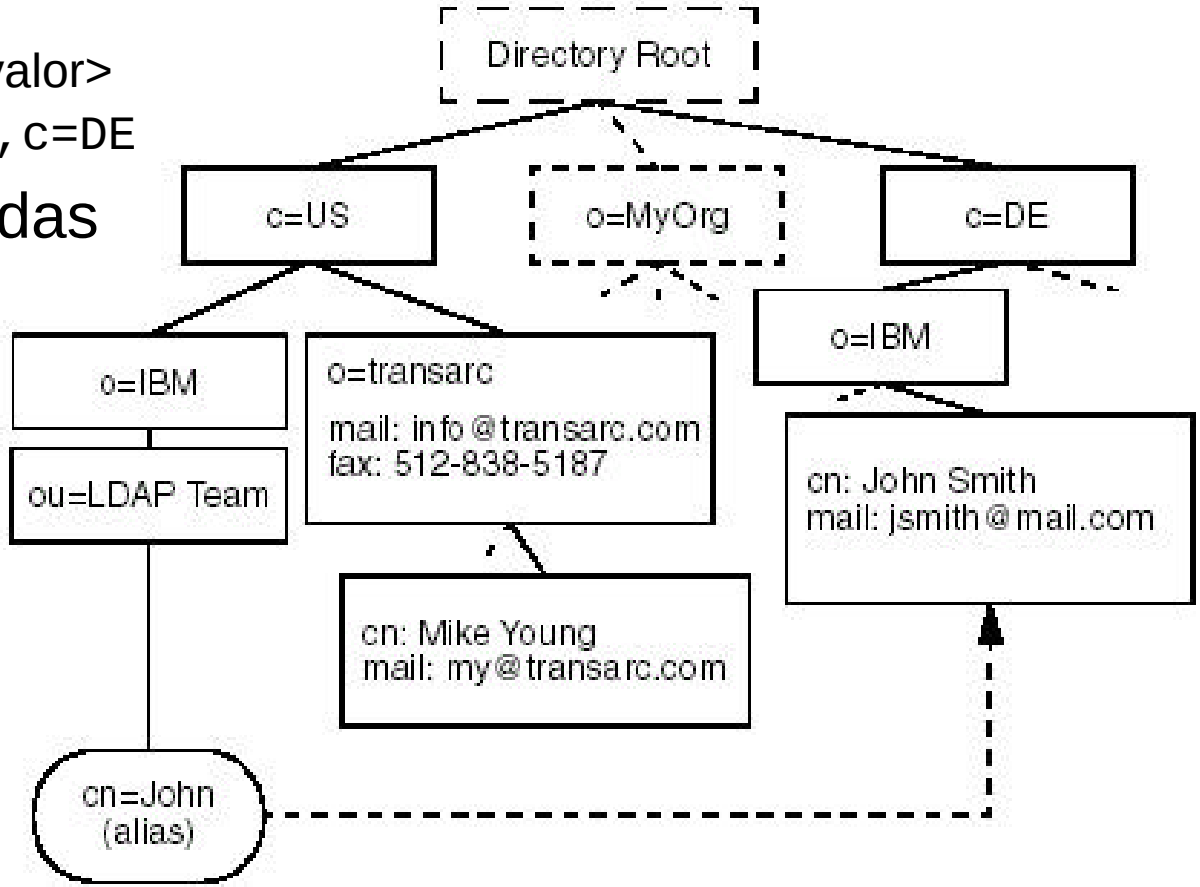
3. LDAP

- Modelo de información
  - Entradas
    - Objetos (personas, servidores, organizaciones)
    - Colección de atributos
  - Tipos atributos
    - Nombre (cn)
    - Apellidos (sn)
    - Teléfono (tel)
  - Esquemas
    - Tipo de objetos y sus atributos
    - Ej: persona necesita atributo apellidos (sn)



3. LDAP

- DN: Nombre Distintivo
  - Identifica a una entrada (único)
  - Secuencia de RDNs
    - <nombre atributo>=<valor>
  - `cn=John Smith,o=IBM,c=DE`
- Organización de entradas
  - Árbol de Información del Directorio (DIT)
  - Jerárquica
  - Según DN
  - Alias apunta
    - Rama
    - Hoja



3. LDAP

- Modelo cliente-servidor
  - Pregunta cliente
  - Respuesta servidor
    - Info demandada
    - Puntero a otra fuente de info (*referrals* v3)
- TCP (v2/v3) o UDP (v3)
- Control de acceso
  - Protección de info: autentificación
    - Anónima, simple (contraseña en claro), Kerberos v4
    - SSL (LDAPv3)

3. LDAP

- Replicación entre servidores LDAP
  - Mediante funcionalidad protocolo LDAP

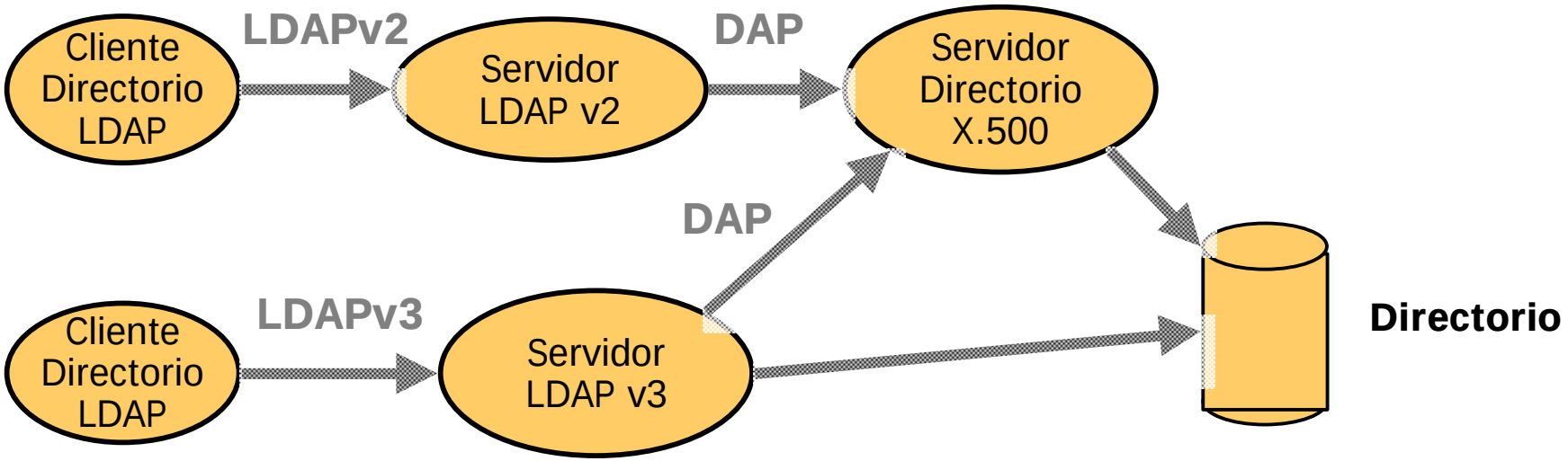
- ldap URL
  - ldap[s]://[<host>[:<port>]] [/ [<dn> [? [<attributes>] [? [<scope>] \
    [? [<filter>] [? <extensions>]]]]]]
  - ldap://ldap.upc.es/o=UPC,c=ES
  - ldap://ldap.upc.es/o=UPC,ou=AC,c=ES?mail

3. LDAP

- Operaciones
  - bind: conexión y autentificación
  - unbind: desconexión
  - search: búsqueda
  - modify / add / delete: modificar / añadir / eliminar una entrada
  - modify RDN
  - compare: comprobar si una entrada tiene un pareja atributo/valor
  - abandon: cancelar una petición pendiente

3. LDAP

- LDAPv3
  - Servidor LDAPv3 puede
    - Implementar el directorio
    - Conversor LDAP/DAP (como LDAPv2)



3. LDAP

- LDAPv3
  - Soporte *referrals*: un servidor devuelve un puntero a otro servidor
  - Seguridad: Autentificación mediante mecanismos SASL (Simple Authentication Security Layer)
    - DIGEST-MD5, CRAM-MD5, S/Key, GSSAPI, Kerberos v4 ...
  - Internacionalización: soporte UTF-8, ISO 10646
  - Extensiones: objetos y operaciones no predefinidas
  - Conexión TCP opcional (bind)

  - Mayor soporte de X.500 que LDAP v2
  - Clientes ya no tan sencillos
  - Ya soportado por bastantes productos

3. LDAP

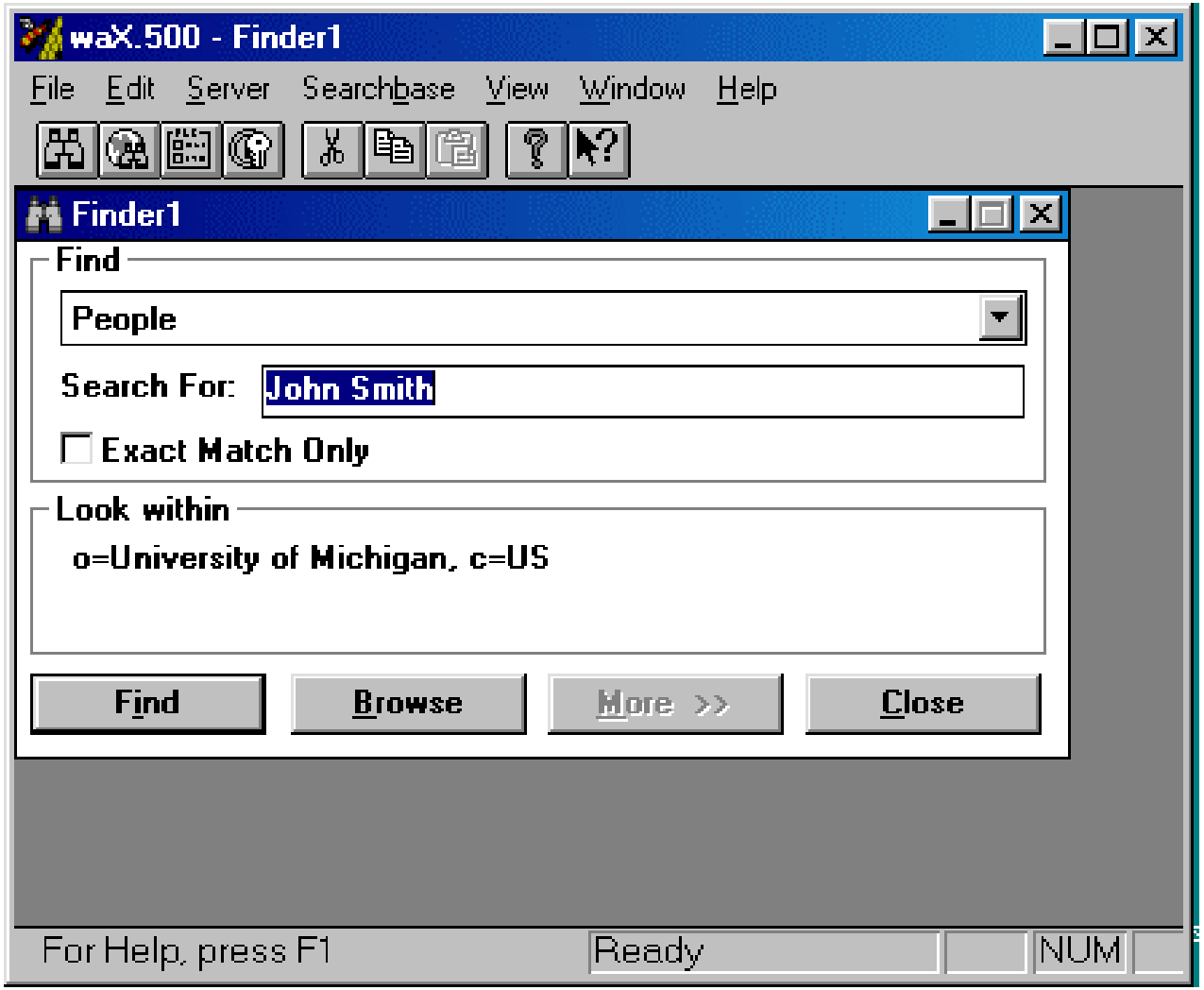
- Relación con UNIX
  - Distribución de datos de configuración
    - Configuración de sendmail (alias, mail homes)
    - Gestión usuarios y contraseñas
    - Servidor de calendario
- Relación con correo: vCard (mime)
  - Transporte de info de directorio sobre correo electrónico

3. LDAP

- Implementaciones de servidores LDAP
  - Dominio público:
    - OpenLDAP (`slapd, slurpd`), Eudora LDAP Directory Server, The JavaLDAP Server Project
  - Comerciales:
    - M-Vault, Netscape Directory Server, Microsoft ActiveDirectory, ...
- http://www.rediris.es/ldap/software/
  - Servidores de directorio
  - Clientes
  - Pasarelas Web-LDAP
  - Herramientas de desarrollo

3. LDAP

- Clientes LDAP



4. LDAP vs X.500

- En común:
  - DIT, DNs, atributos, búsquedas por filtros, ...
- X.500: DAP: protocolo de acceso a directorio
  - Especificación muy detallada
  - Sobre OSI
  - Muchos recursos (“pesado”)
- LDAP: acceso ligero a X.500
  - TCP/IP
  - Clientes sencillos

4. LDAP vs X.500

- El directorio X.500: ~1,5 M. entradas (9/1998)
  - Crecimiento mucho menor que el de Internet
- Faltan autoridades de registro internacionales
  - “Organization” (o) deben estar registrados.
- Algunas razones
  - Complejidad de los protocolos
  - Recursos necesarios para implementar y soportar el servicio
  - Algo/demasiado abstracto
  - Preocupación por la seguridad
  - Privacidad y cultura: publicar lo que solía ser privado

5. ACAP

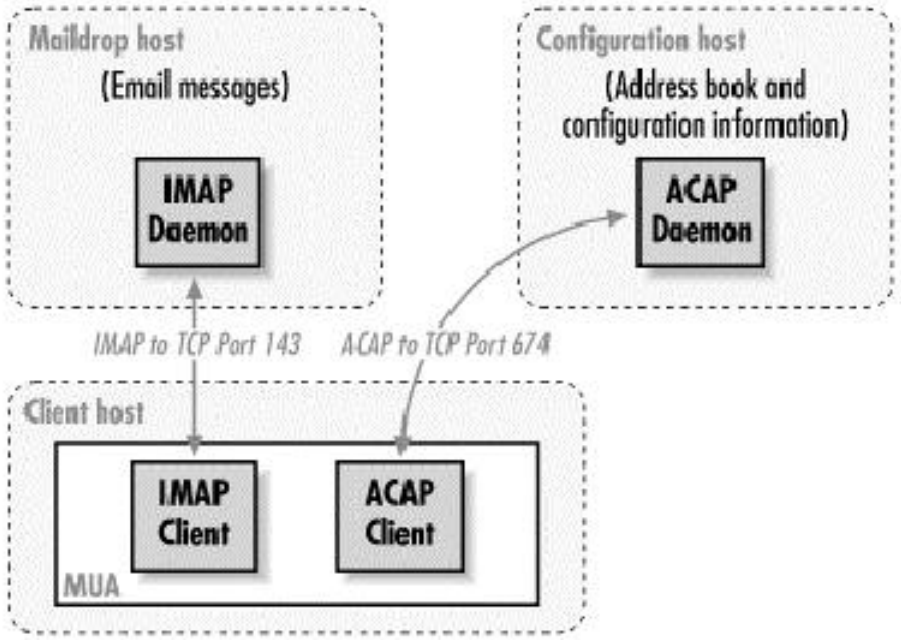
- Application Configuration Access Protocol
- Derivado de IMAPv4
- Almacenamiento y acceso remoto de información:
  - Preferencias/opciones de configuración de aplicaciones
    - Configuración correo, ...
  - Datos personales
    - Listas de direcciones de correo, diccionarios, bookmarks, listas de subscripción (news), ...
  - Perfiles de usuarios móviles (*roaming*)
    - N puntos de acceso x N usuarios
- Enfocado a aplicaciones clientes de Internet
  - Eudora v4 lo soporta

5. ACAP

- Motivado por evolución Internet (1995)
  - Acceso desde trabajo, casa, viajes, ...
  - Varios usuarios/máquina
  - Varias máquinas/usuario
  - Disminución nivel experiencia manejo computadores
  - Movilidad
    - Geográfica
    - Usuarios
    - SO, aplicación
- No es un servicio de directorio

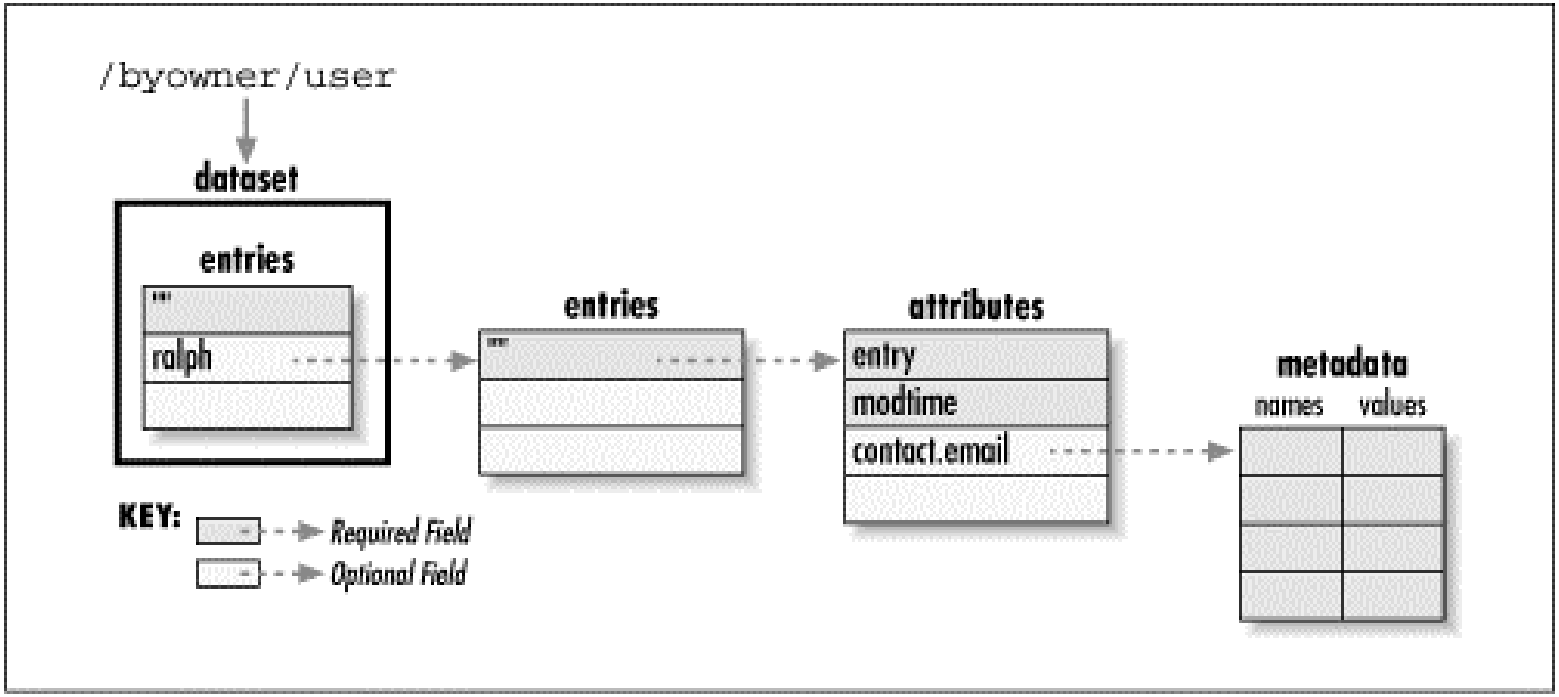
5. ACAP

- Protocolo cliente-servidor
  - Comandos del cliente - respuestas del servidor
- Sintaxis y estructura similar a IMAP4
- Conjuntos de datos predefinidos
  - listas de @ de correo
  - bookmarks, ...



5. ACAP

- Almacenamiento de conjunto de entradas en un servidor
  - Entrada: conjunto de pares atributo/valor



5. ACAP

- Servicios de directorio (LDAP, X.500, ...)
  - Control del servidor
  - Búsqueda rápida de información pública y “cuasi-estática”
  - Funcionamiento on-line
- ACAP
  - Control del cliente/usuario
  - Datos más dinámicos
  - Funcionamiento off-line (cache-local)

Bibliografía

- General
  - Understanding LDAP
    - http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg244986.html
  - http://java.sun.com/products/jndi/tutorial/ldap/
  - http://www.rediris.es/ldap/
- X500
  - http://www.isi.salford.ac.uk/staff/dwc/Version.Web/Contents.htm
- LDAP
  - http://www.umich.edu/~dirsvcs/ldap/doc/
- ACAP
  - http://asg.web.cmu.edu/acap/
  - http://www.oreilly.com/catalog/progintemail/chapter/ch12.html