Servicios basados en LDAP :

Migración desde X.500

Alfonso López Murcia
alfonso@dif.um.es

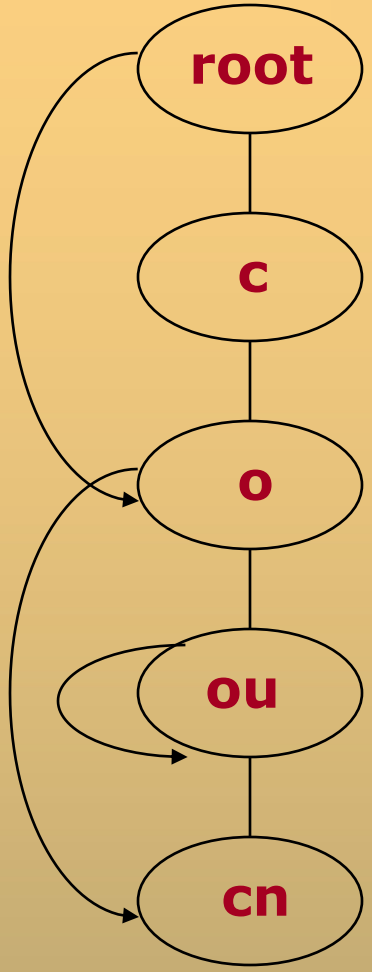
CONTENIDOS

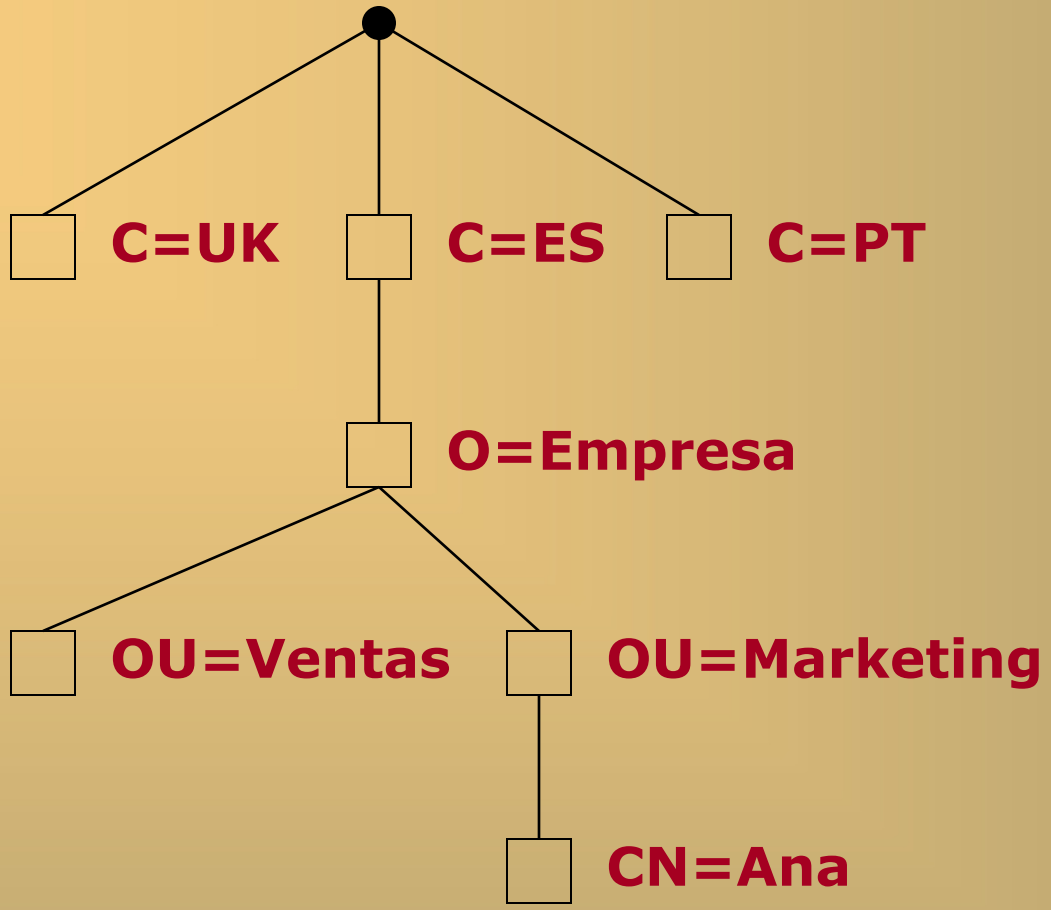
- ⇨ CARACTERISTICAS DE X.500 Y LDAP
- ⇨ NUEVO ESQUEMA BASADO EN DOMINIOS
- ⇨ PASO DE X.500 A LDAP
- ⇨ NUEVOS SERVICIOS

EL DIRECTORIO X.500

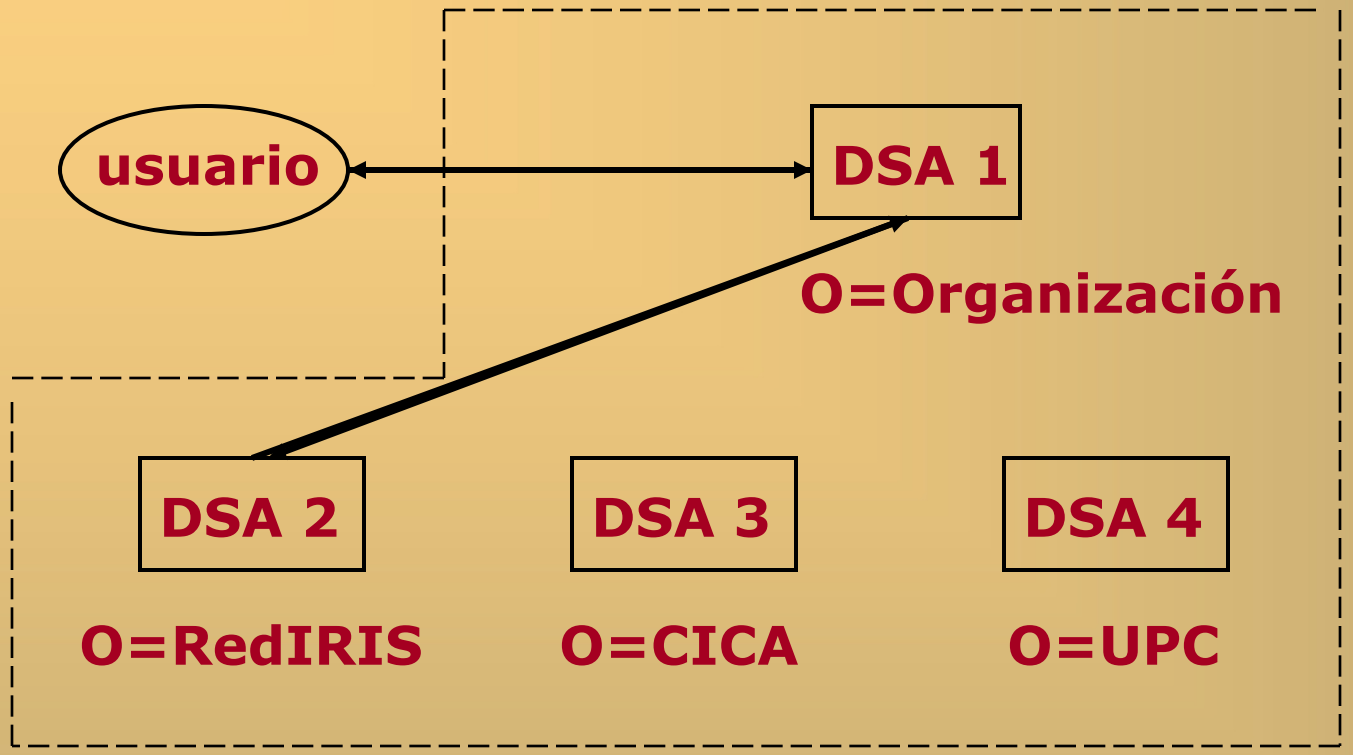
- Protocolos OSI
- Recomendaciones X.500
- Esquema X.521 basado en criterios geopolíticos
- Trabajo de los servidores: "chaining"

ESQUEMA X.521





CONSULTA X.500



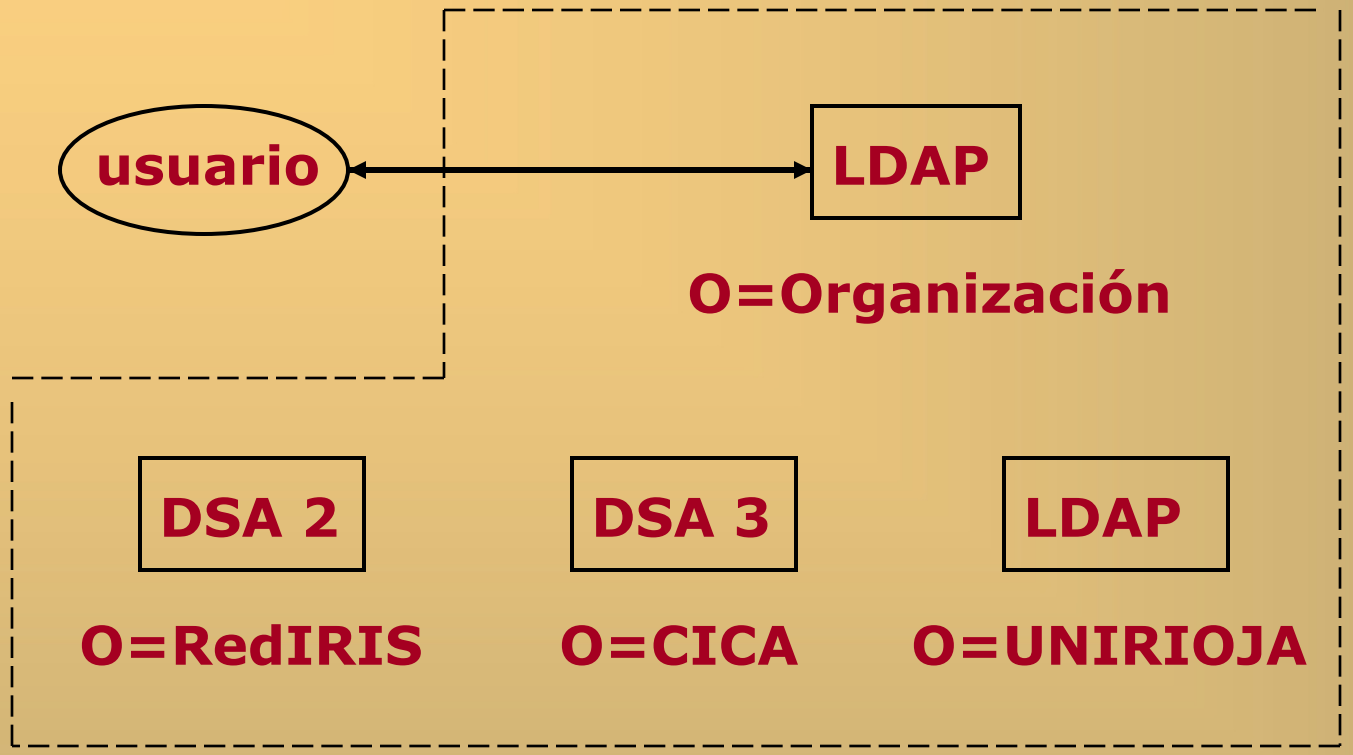
DIRECTORY ACCESS PROTOCOL (DAP)

DIRECTORY SYSTEM PROTOCOL (DSP)

ALTERNATIVA TCP/IP

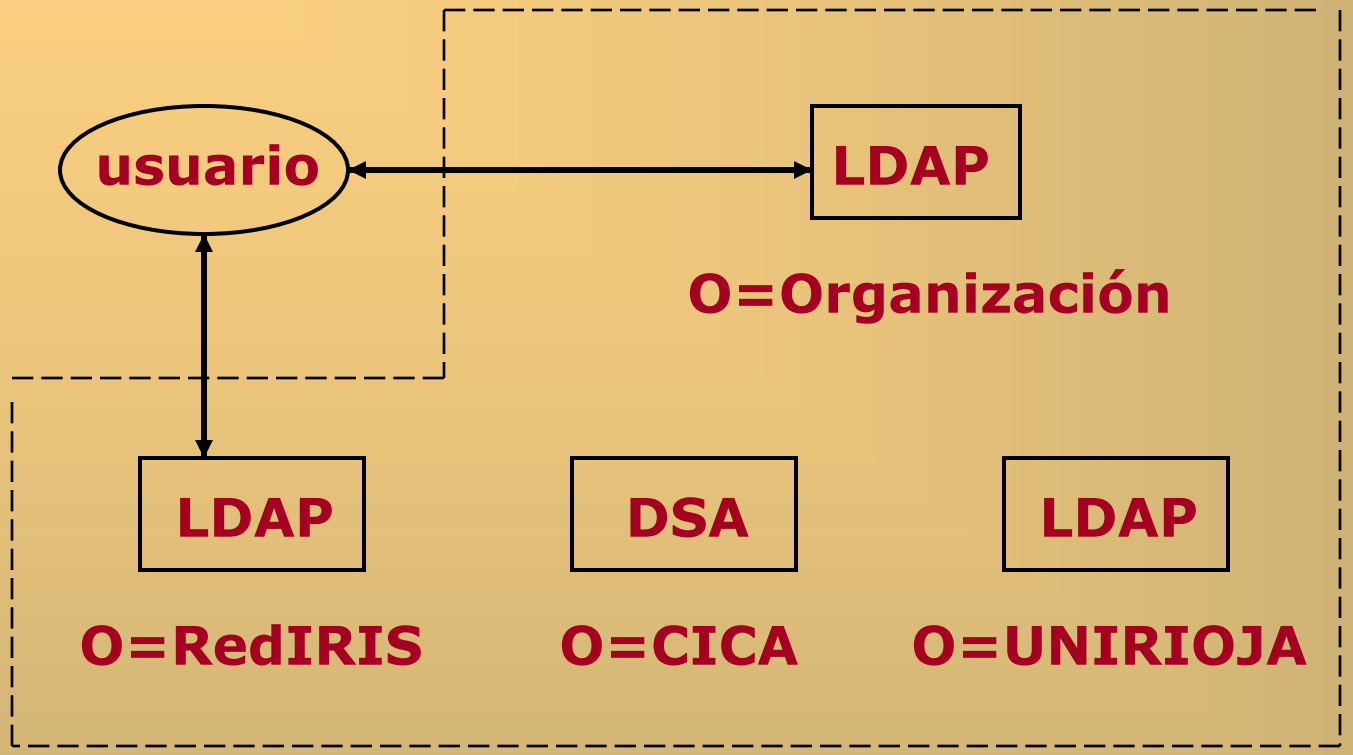
- Los protocolos OSI son pesados y poco eficientes
- LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP), RFC 1777
- Servidores LDAP

CONSULTA LDAP



LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

CONSULTA LDAPv3

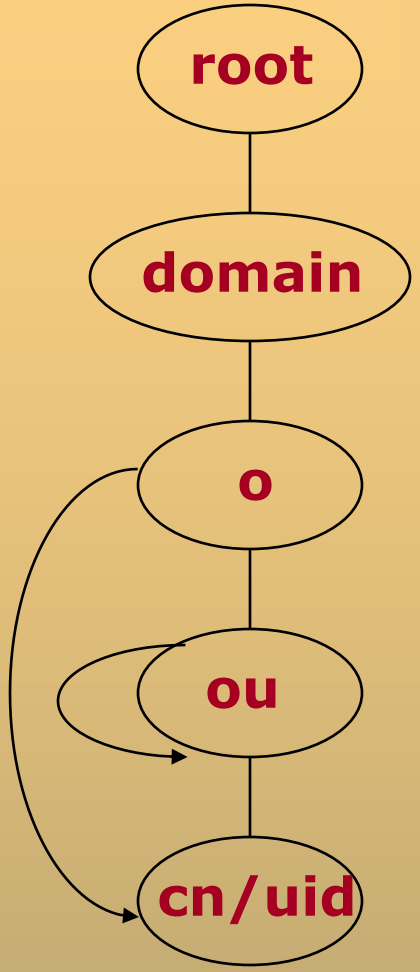


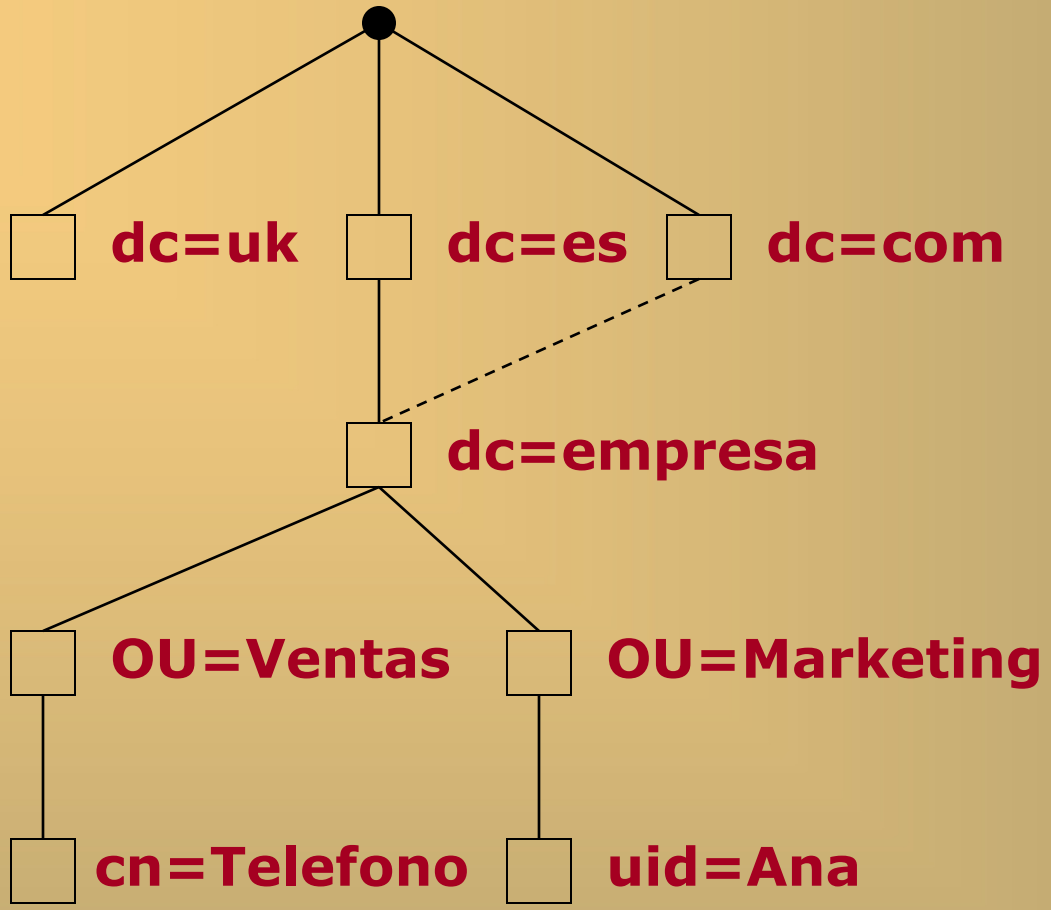
LDAPv3 RFC 2251- REFERENCIA

CONSECUENCIAS

- Sustituir servidores X.500 por LDAP
- Como Internet se basa en dominios, pues vamos a reflejarlo en el Directorio: RFC 2377

ESQUEMA RFC 2377

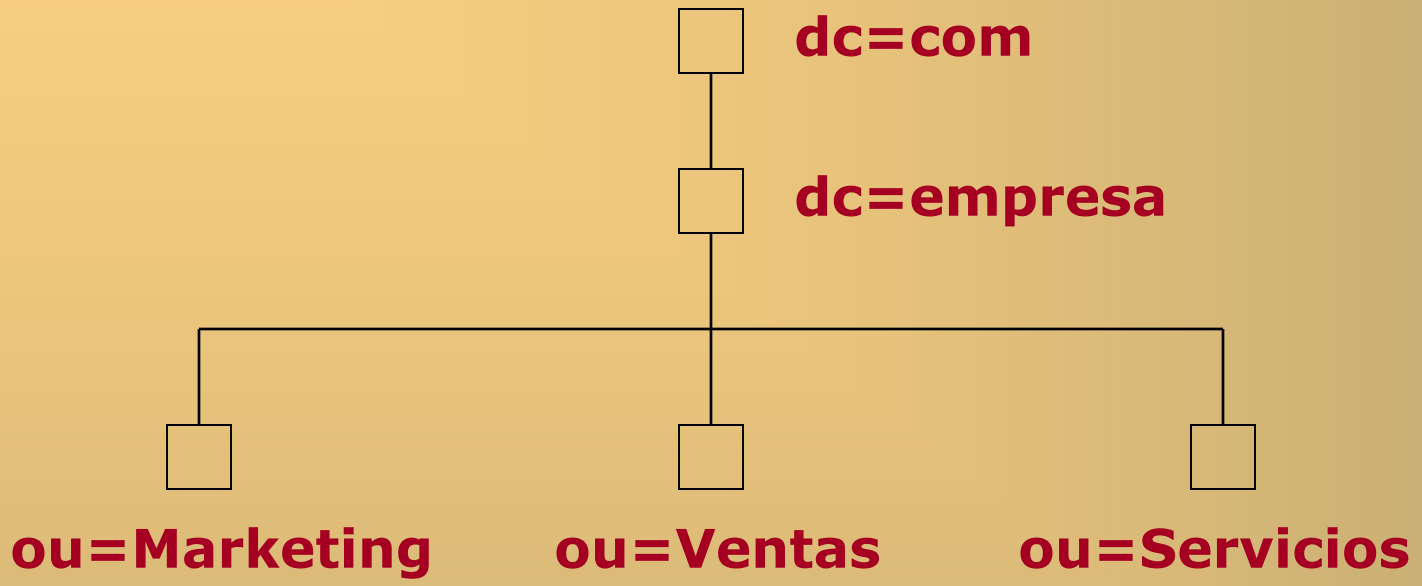




LDIF ORGANIZACION

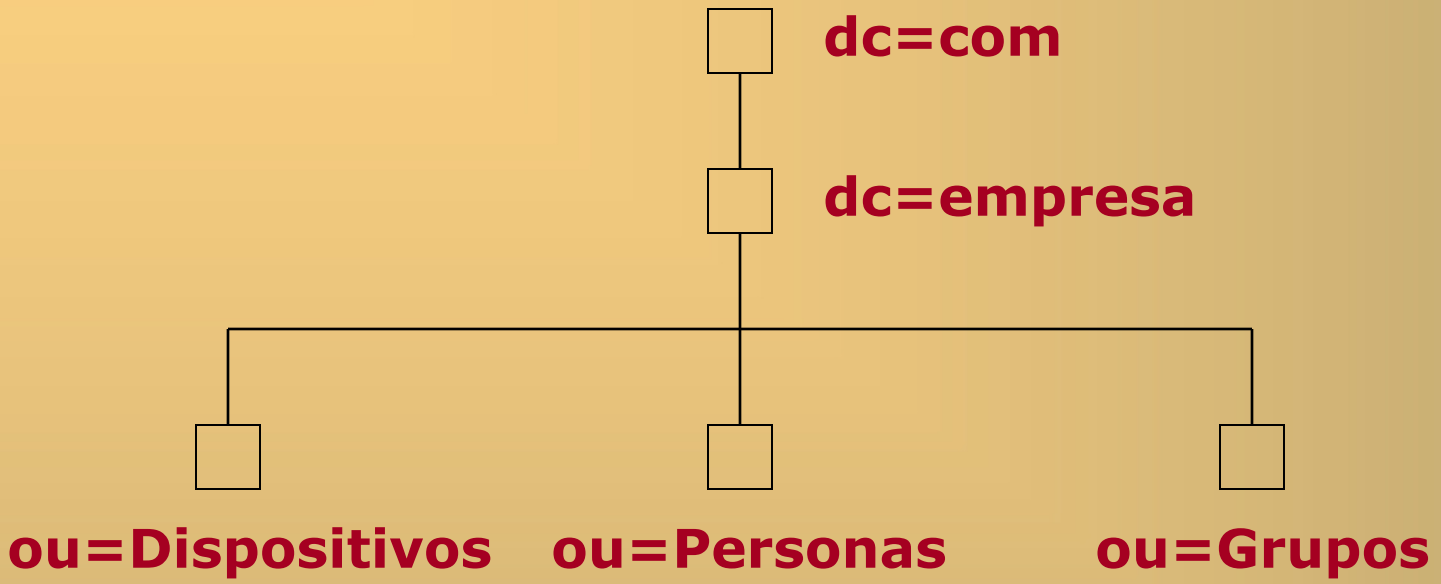
dn: dc=empresa, dc=com
objectclass: organization
objectclass: **dcObject**
objectclass: domainRelatedObject
objectclass: labeledURIObject
o: Empresa Familiar
dc: empresa
associatedDomain: empresa.com
labeledURI: http://www.empresa.com Web Emp
…

ESPACIO DE NOMBRES (I)



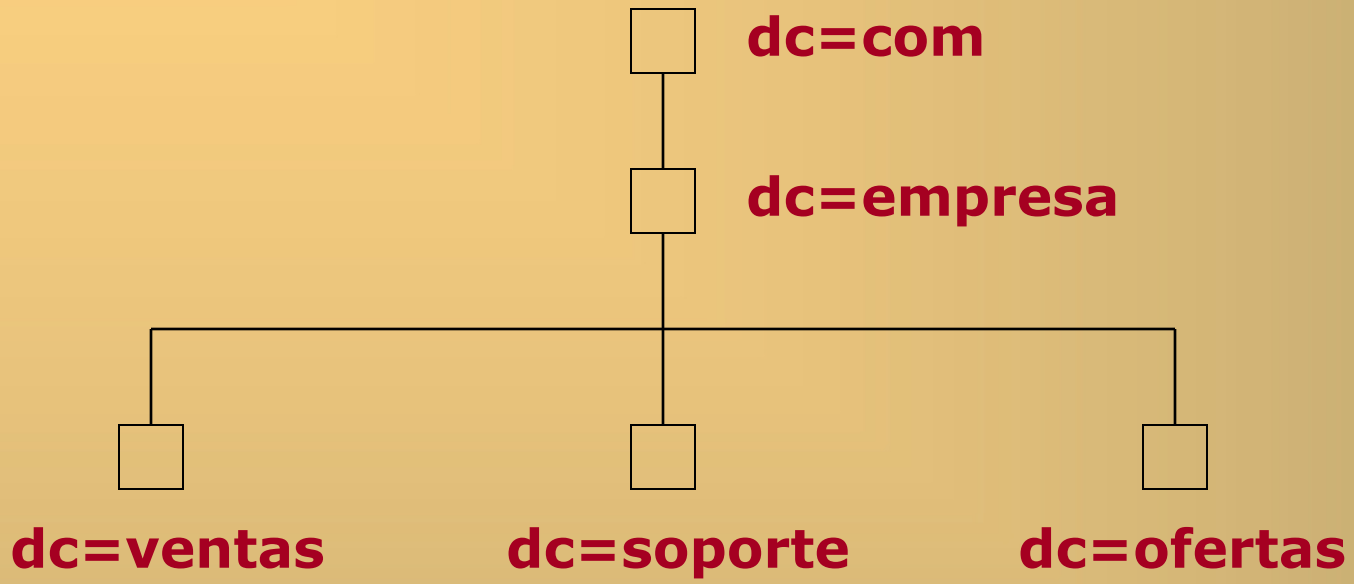
Basado en la organización

ESPACIO DE NOMBRES (II)



Basado en los objetos

ESPACIO DE NOMBRES (III)



Basado en dominios

FORMATO ENTRADA

dn: uid=ana, dc=empresa, dc=com
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: account
cn: Ana Romero Velázquez
sn: Romero Velázquez
mail: ana@empresa.com
ou: mailing
…

MIGRACION

- Elegir un espacio de nombres
- Extraer entradas (LDIF) y volcarlas al servidor LDAP
- Determinar restricciones
- Esquema mixto:

  o=organización,c=es

  dc=organización,dc=es

MANTENIMIENTO REFERENCIAS

- Referencias generadas a partir de registros SRV del DNS:

_ldap._tcp.uni.es IN SRV 0 0 389 ldap.uni.es.

producirá la referencia

ldap://ldap.uni.es:389/

¿DEBO TENER UN SERVIDOR LDAP?

- Certificados
- Perfiles móviles (roaming)
- Autenticación en UNIX
- Autenticación en UNIX y Windows (no probado)

ROAMING EN NETSCAPE (I)

- El entorno del usuario en el navegador Netscape está en un servidor LDAP
- Guía (OpenLDAP 1.2.x)

  http://www.um.es/~linux/ldap
- Esquema incluido en 2.0.x

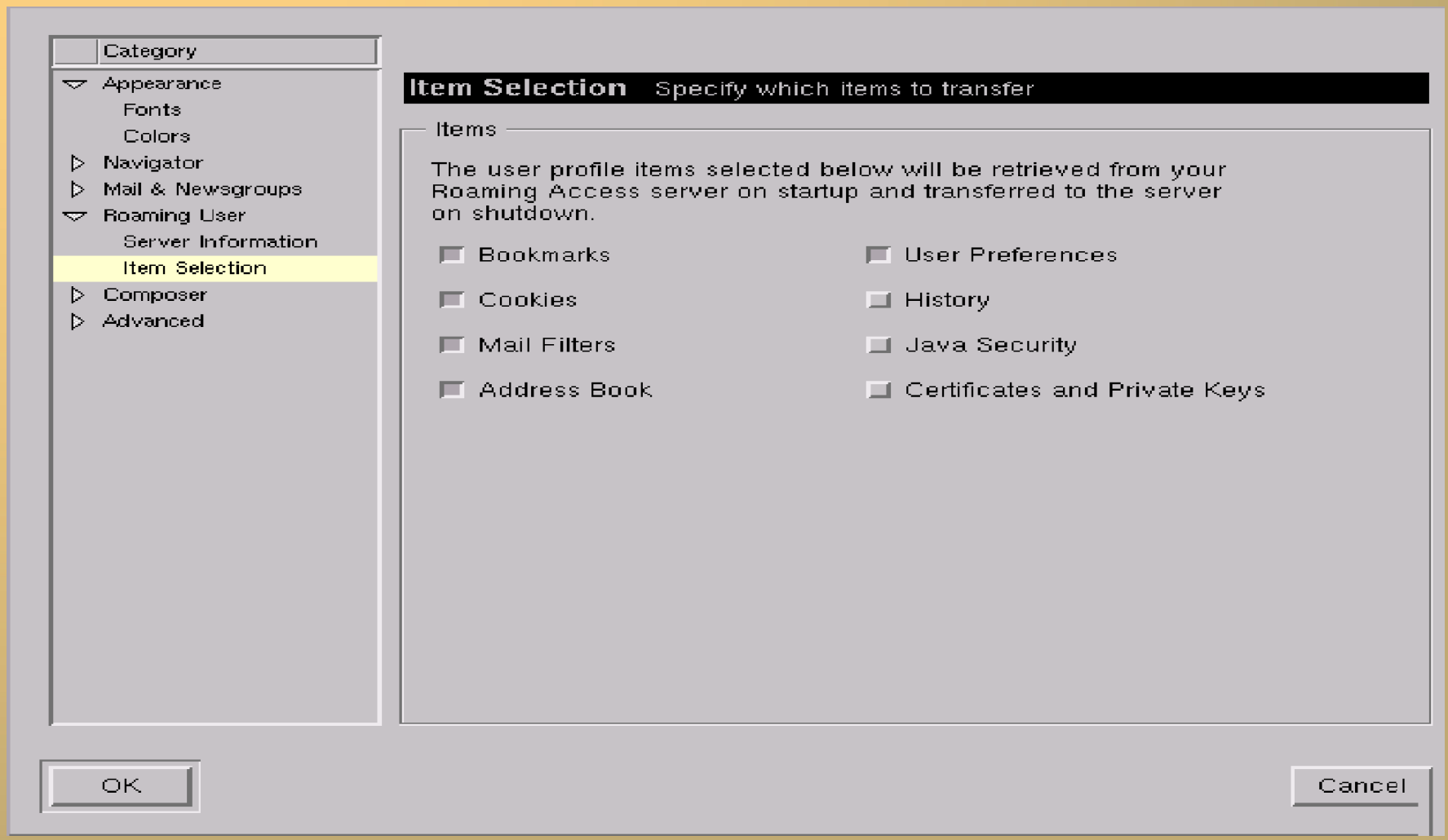
ROAMING EN NETSCAPE (II)

dn: ou=Roaming, dc=uni, dc=es
objectclass: organizationalUnit
ou: Roaming

dn: cn=Profe Emerito, ou=Dept, dc=uni, dc=es
objectclass: person
cn: Profe
sn: Emerito
userpassword: secret

dn: nsLIProfileName=Profe Emerito, ou=Roaming, dc=uni, dc=es
objectclass: nsLIProfile
owner: cn=Profe Emerito, ou=Dept, dc=uni, dc=es

ROAMING EN NETSCAPE (III)



AUTENTICACION EN UNIX (I)

- PAM, utilidades PADL y RFC 2307 sustituimos NIS
- Guía (OpenLDAP 1.2.x) http://www.um.es/~linux/ldap
- Esquema incluido en 2.0.x

AUTENTICACION EN UNIX (I)

dn: uid=ana, dc=uni, dc=es
uid: ana
cn: Ana Romero Velazquez
objectClass: account
objectClass: posixAccount
userPassword: {crypt}V479CQrvyweWQ
loginShell: /bin/bash
uidNumber: 500
gidNumber: 100
homeDirectory: /home/ana
gecos: Ana Romero Velazquez

VIAS FUTURAS

- Autenticación Windows y Unix. Howto de Ignacio Coupeau
- Referencias en el DNS
- Aumento de la seguridad
- Colaboración con el Comité de Migración

Gracias por su atención