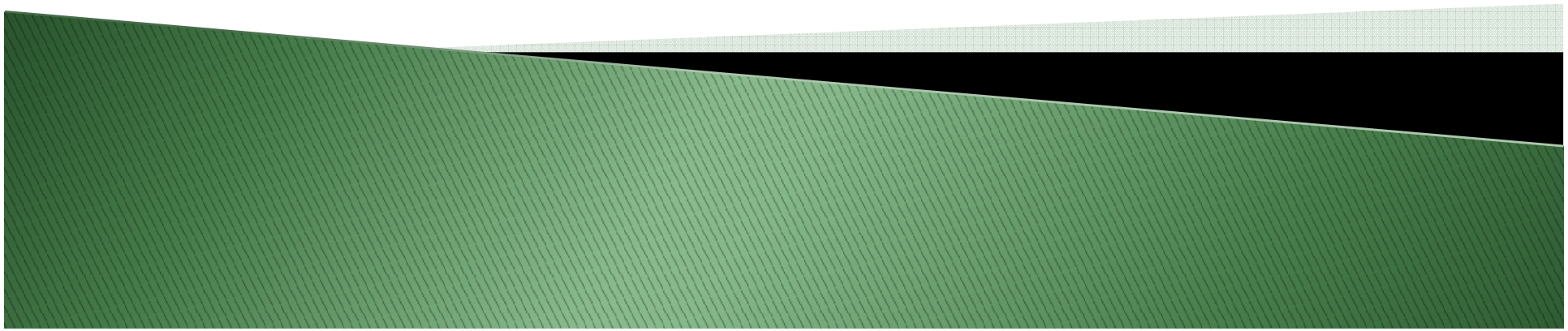
Unidad 9

Servicios de directorio. LDAP

Despliegue de aplicaciones web



Índice

- Servicios de directorio.
  - Introducción.
  - X.500.
  - Características.
- LDAP
  - Introducción.
  - Versiones.
  - Características
  - Modelo de datos.
    - DIT

Índice

Índice

Servicios de directorio
Introducción

- Sistema software que ofrece servicios de gestión y acceso a un conjunto de información (directorio).
- Búsqueda de información basada en nombres.

Servicios de directorio
Introducción

- Termino “ambiguo”, según la definición
  - La sistemas de ficheros “son servicios directorio”.
  - La bases de datos “son servicios de directorio”.
  - DNS en un servicio de directorio.
  - …

- Se suele utilizar el termino “**servicio de directorio**” para referirse a los servicios basados en los estándares X.500.

Servicios de directorio
X.500

- Conjunto de estándares sobre servicios de directorio definidos por la ITU (http://www.itu.int/es/).
- Define
  - Protocolos
    - DAP (*Directory Access Protocol*)
    - DSP (*Directory System Protocol*)
    - DISP (*Directory Information Shadowing Protocol*)
    - DOP (*Directory Operational Bindings Management Protocol*)
  - Modelos de datos

Servicios de directorio
Características

- Arquitectura cliente/servidor.
- Organización jerárquica e los datos.
- Estructura flexible.
- Muchas lecturas y pocas escrituras -> Optimizados para lecturas.
- Alto rendimiento (miles de accesos por segundo).
- Distribuidos.

Servicios de directorio
Características

- Webs
  - http://es.wikipedia.org/wiki/Servicio_de_directorio
  - http://en.wikipedia.org/wiki/Directory_service
  - http://es.wikipedia.org/wiki/X.500
  - http://en.wikipedia.org/wiki/X.500

LDAP
Introducción

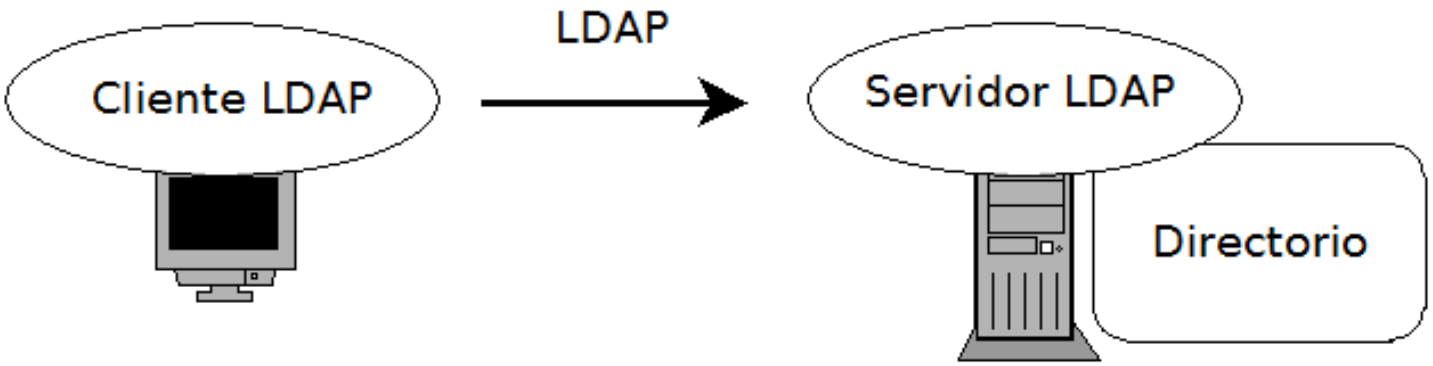
- X.500
  - Protocolo DAP para acceder a los servicio de directorio a través de una red.
  - DAP se basaba en la pila de protocolos OSI.
- LDAP
  - Definido por la ITU con el objetivo de ofrecer la misma funcionalidad que DAP pero sobre la pila de protocolos TCP/IP.
  - Simplifica DAP.
- La terminología X500 y LDAP es similar.

LDAP
Versiones

- LDAPv2.
  - Obsoleto
- LDAPv3.
  - Remplaza a LDAP v2.
  - Más rápido
  - Más opciones de autenticación
  - SSL/TLS y Certificados digitales X.509.
  - Esquemas.

LDAP
Características

- Técnicamente LDAP es solo un protocolo que define como acceder a un directorio de datos.



LDAP
Características

- Necesariamente, también define y describe
  - Como los datos son representados en el directorio.
  - Como los datos son cargados (importados) y exportados en/del directorio (LDIF).
- LDAP NO define como los datos son almacenados y manipulados.
- Optimizado para consultas.
- No transaccional (no hay *roolback*).

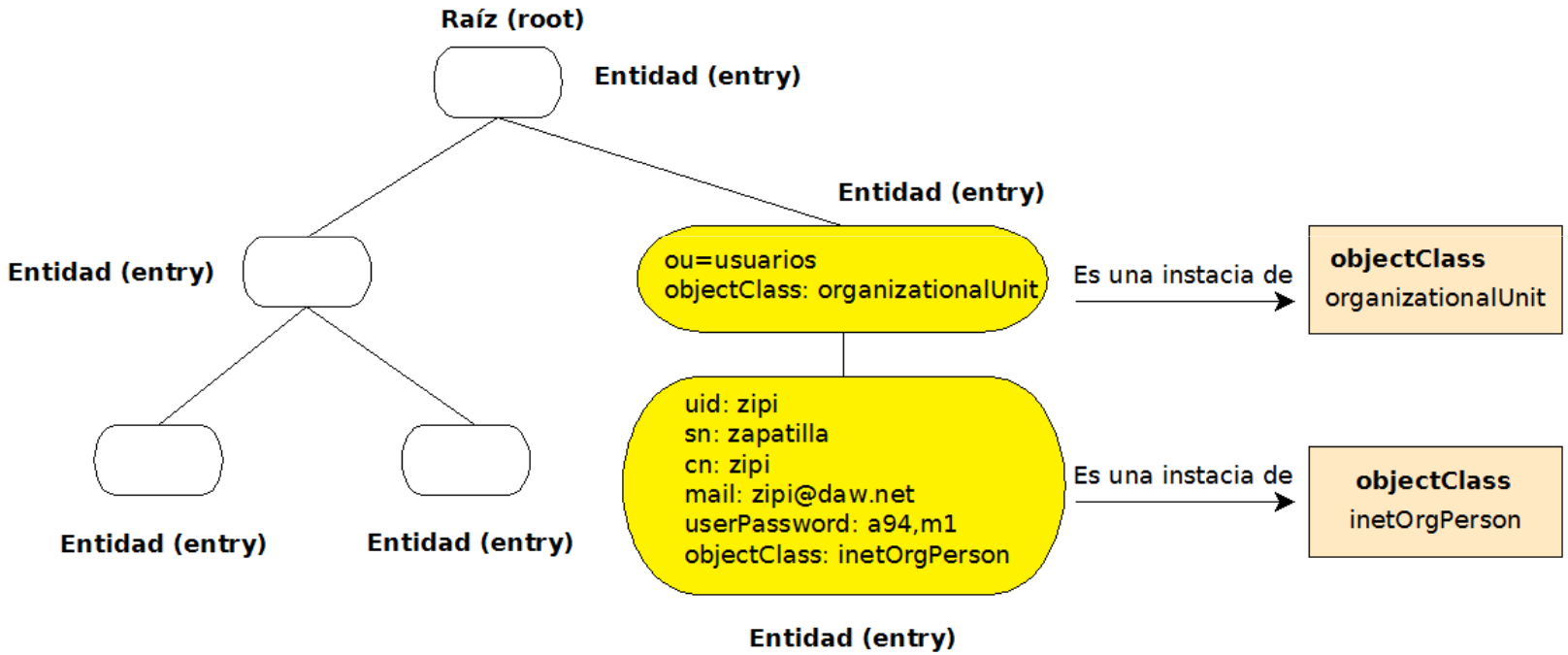
LDAP
Características

- **Modelo de información (modelo de datos)**
  - Define la estructura de la información almacenada en el directorio.
- **Modelo de nombrado**
  - Como nombra y se identifica a la información almacenada en el directorio.
- **Modelo funcional**
  - Operaciones sobre la información: búsquedas, lecturas, escrituras y modificaciones.
- **Modelo de seguridad**
  - Control de acceso.
  - Quien y que puede hacer en el directorio.

LDAP
Modelo de datos. DIT

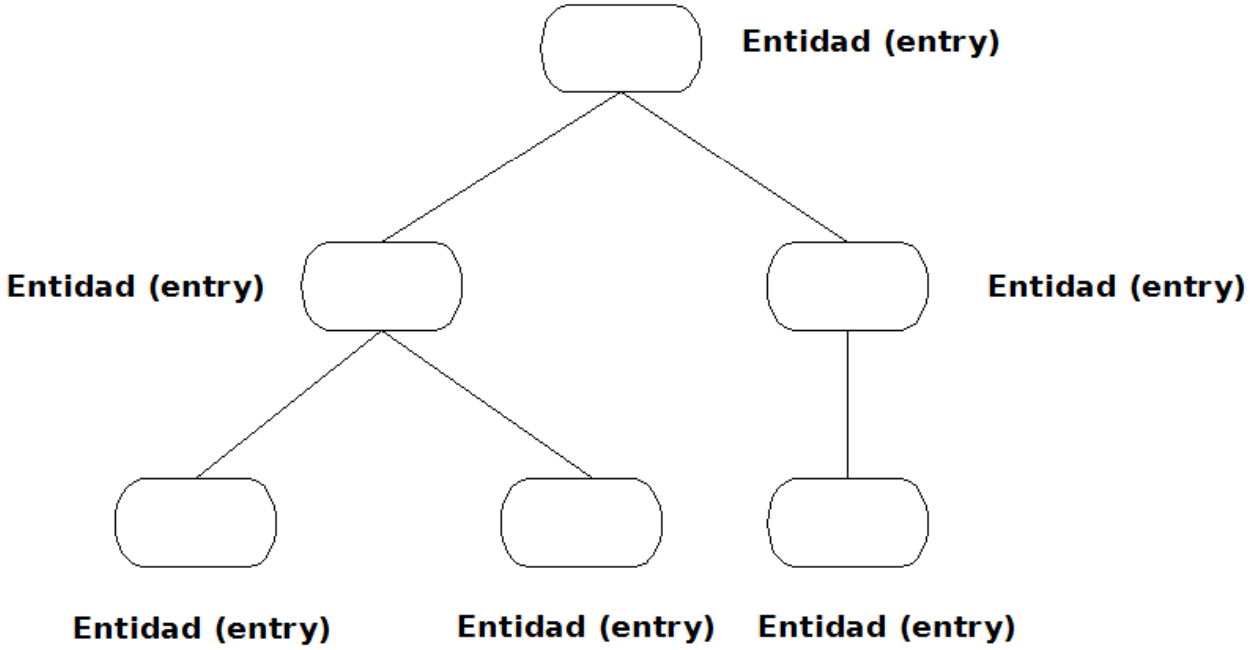
- La información de un directorio LDAP esta formada por un conjunto de objetos – entradas (*entry*) – organizadas jerárquicamente.
- La estructura resultante se denomina DIT (*Data Information Tree*).
- La entrada más alta del árbol se denomina normalmente raíz (*root*).

LDAP
Modelo de datos. DIT



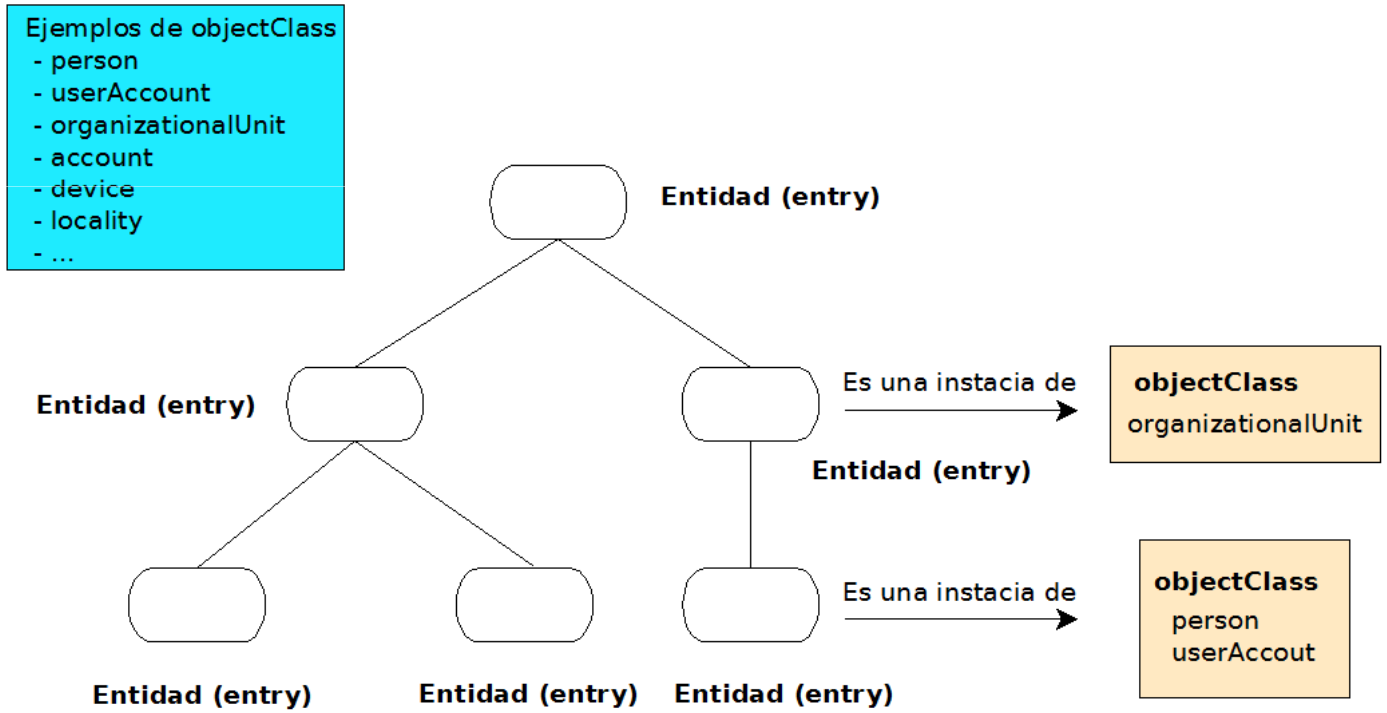
LDAP
Modelo de datos. Entidades (*entry*)

- Conjunto de objetos que forma el directorio LDAP organizados jerárquicamente (DIT).



LDAP
Modelo de datos. *objectClass*

- Cada entidad *(entry)* es una instancia de una o varias clases (*objectClass*).



LDAP
Modelo de datos. *objectClass*

- Cada *objectClass* tiene un **nombre** y define uno varios **atributos** y sus **tipos de datos.**
  - Ejemplos de **objectClass**

Nombre: **account**
Atributos:
userid (obligatorio) (*)
description
localityName
organizationName
…

Nombre: **person**
Atributos:
cn (common name) (*)
sn (surname) (*)
telephoneNumber
organizationName
…

    - * -> Atributos obligatorios (**MUST**)
    - El resto opcionales (**MAY**)

LDAP
Modelo de datos. *objectClass*

DESC	• RFC2256: a person
MAY	• userPassword • telephoneNumber • seeAlso • description
MUST	• sn • cn
NAME	• person
objectClass	• top • synthetic_JXplorer_schema_object
OID	• 2.5.6.6
SUP	• top

MAY	• description • seeAlso • localityName • organizationName • organizationalUnitName • host
MUST	• userid
NAME	• account
objectClass	• top • synthetic_JXplorer_schema_object
OID	• 0.9.2342.19200300.100.4.5
SUP	• top

LDAP
Modelo de datos. *objectClass*

- Los *objectClass* son por lo tanto colecciones de atributos.
  - Obligatorio (*MUST*)
  - Opcional (*MAY*)
- Los *objectClass* puede formar parte de una jerarquía y heredar los atributos de sus padres.
- Se definen en **esquemas** (se explican posteriormente).

LDAP
Modelo de datos. *objectClass*

- Los *objectClass* pueden ser de tipo
  - STRUCTURAL
    - Usados para crear entidades.
  - AUXILIARY
    - Añadidas en entidad existentes (que tienen al menos un *objectClass* STRUCTURAL)
  - ABSTRACT
    - Para definir jerarquías de *objectClass*.

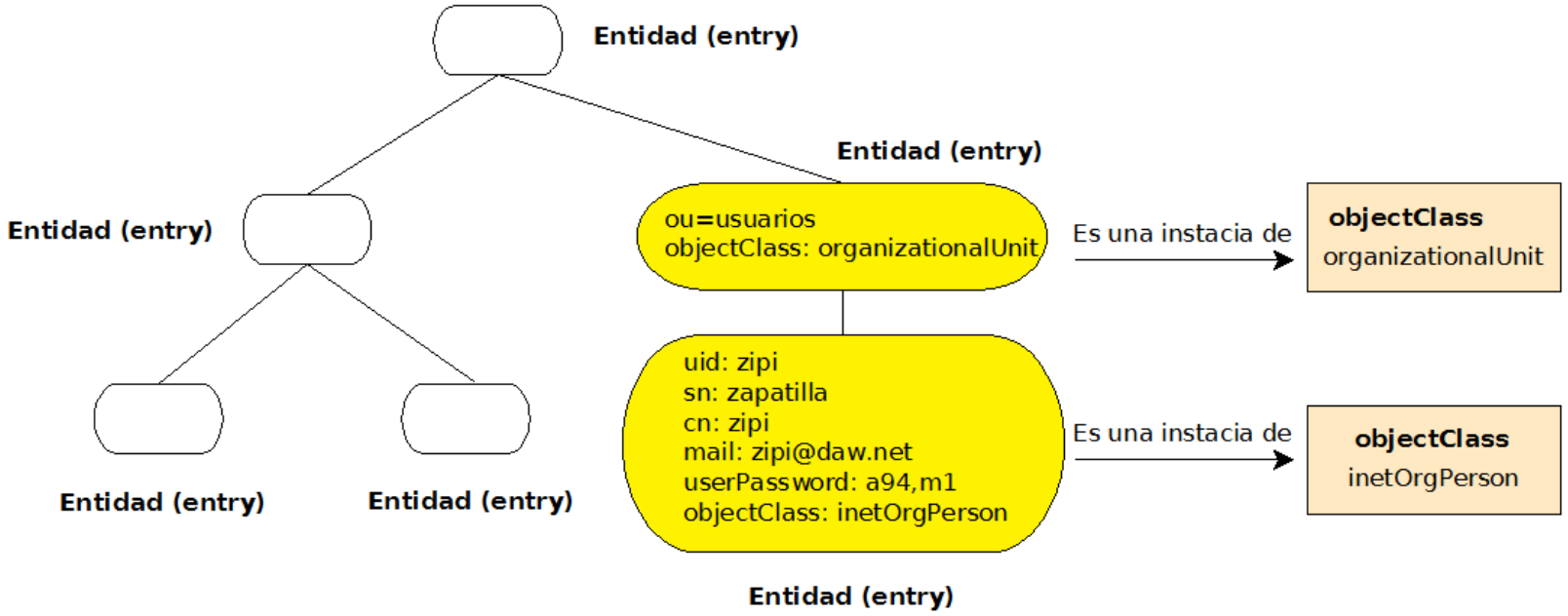
- Web (ejemplos de *objectClass*).
  - http://www.zytrax.com/books/ldap/ape/

LDAP
Modelo de datos. *objectClass*

- Las entidades
  - Deben pertenecer a un (uno y solo uno) *STRUCTURAL objectClass*.
  - Pueden pertenecer a uno o varios *AUXILIARY objectClasses.*
  - Pueden pertenecer solo a un *ABSTRACT objectClass*.

LDAP
Modelo de datos. Atributos

- En función de los *objectClass* a los que pertenezcan (sean instancias de) las entidades tendrán **valores** para los **atributos.**



LDAP
Modelo de datos. Atributos

- En las entidades se definen el atributo especial *objectClass* que contiene como valor el/los *objectClass(es)* a los que pertenece la entidad.

LDAP
Modelo de datos. Atributos

- Todos los atributos son miembros de uno mas *objectClass(es).*
- Cada atributo define un tipo de datos que puede contener.
- Los atributos pueden ser opcionales (MAY) o obligatorios (MUST) dependiendo de la *objectClass.*
  - Un atributo puede ser obligatorio en una *objectClass* y opcional en otra.

LDAP
Modelo de datos. Atributos

- Los atributos puede tener uno o varios valores.
- Los atributos tienen nombres y a veces abreviaturas.
  - Ejemplo: **cn** es una abreviatura de **commonName**.
- En cada nivel de la jerarquía los datos contenidos en los atributos pueden ser usados para identificar a la entrada (*entry)*.

LDAP
Modelo de datos. Esquemas (*Schemas*)

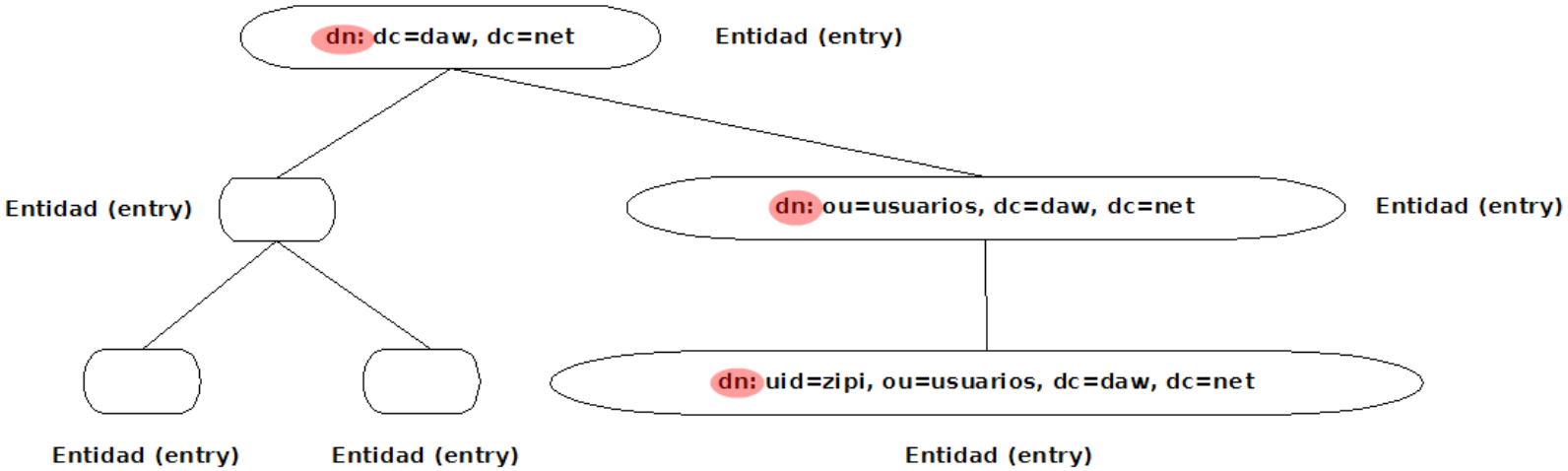
- Los **esquemas** (*schemas*) son paquetes que definen:
  - *objectClass* y y atributos.
  - Un atributo definido en un esquema puede ser usado por o*bjectClass* de otros esquemas.
  - Podemos crear nuestros esquemas propios con los *objectClass* que nos interesen.
- Web (ejemplos de esquemas)
  - http://www.zytrax.com/books/ldap/ape/

LDAP
Modelo de datos. Esquemas (*Schemas*)

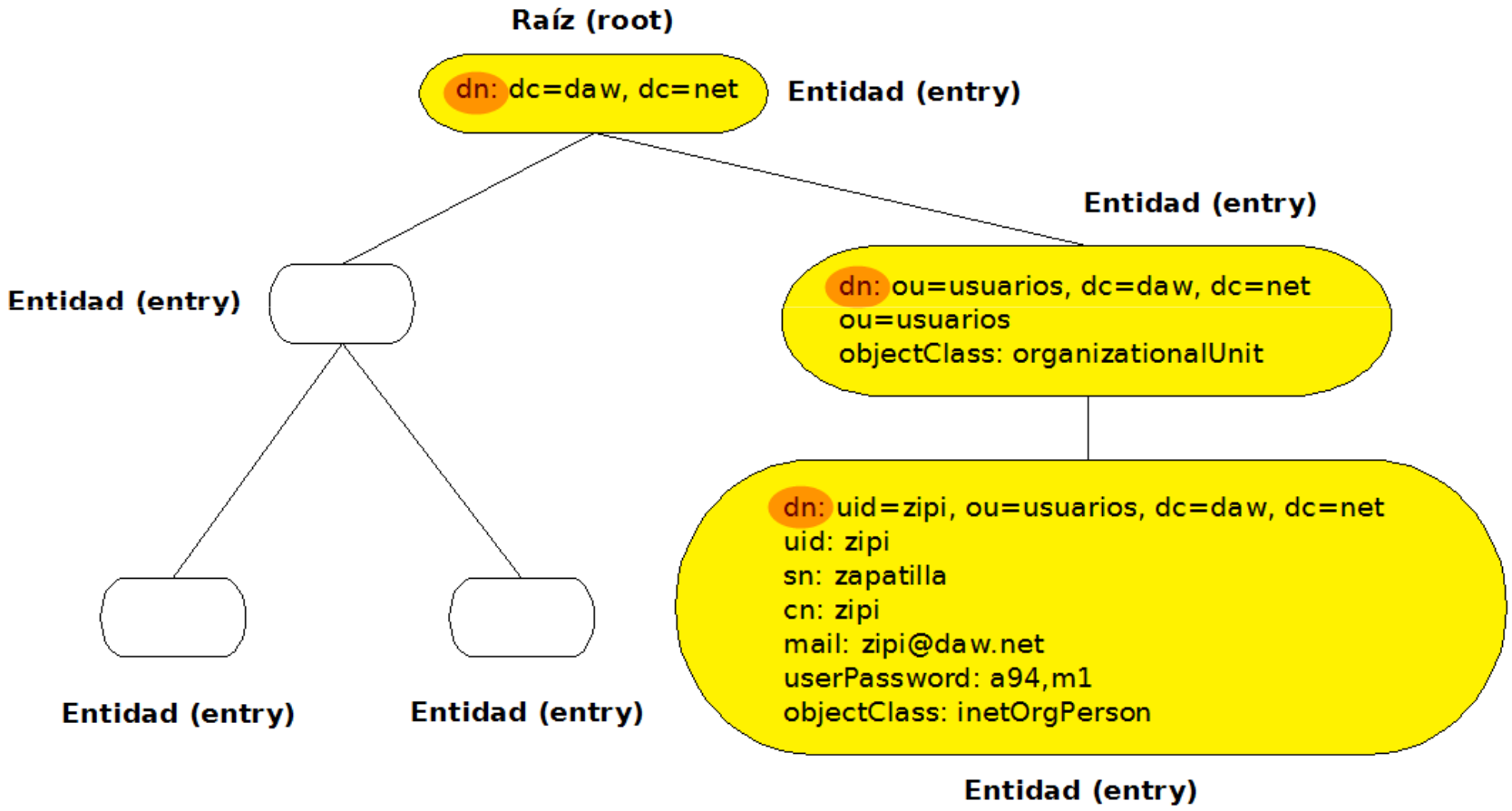
```
objectclass ( 2.5.6.6 NAME 'person' SUP top STRUCTURAL
  MUST ( sn $ cn )
  MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )

objectclass ( 2.5.6.7 NAME 'organizationalPerson' SUP person STRUCTURAL
  MAY ( title $ x121Address $ registeredAddress $ destinationIndicator $
   preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
   telephoneNumber $ internationaliSDNNumber $
   facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $
   postalAddress $ physicalDeliveryOfficeName $ ou $ st $ l ) )
```

LDAP
Modelo de nombrado

- Define como se nombra y se identifica a la información almacenada en el directorio.
- La entradas se organizan el DIT en base a su DN (*Distinguished Name*).

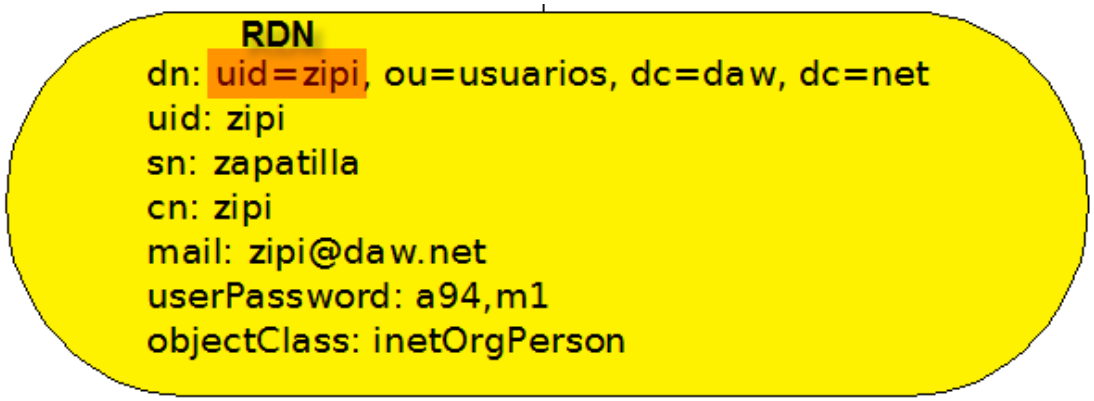


LDAP
Modelo de nombrado



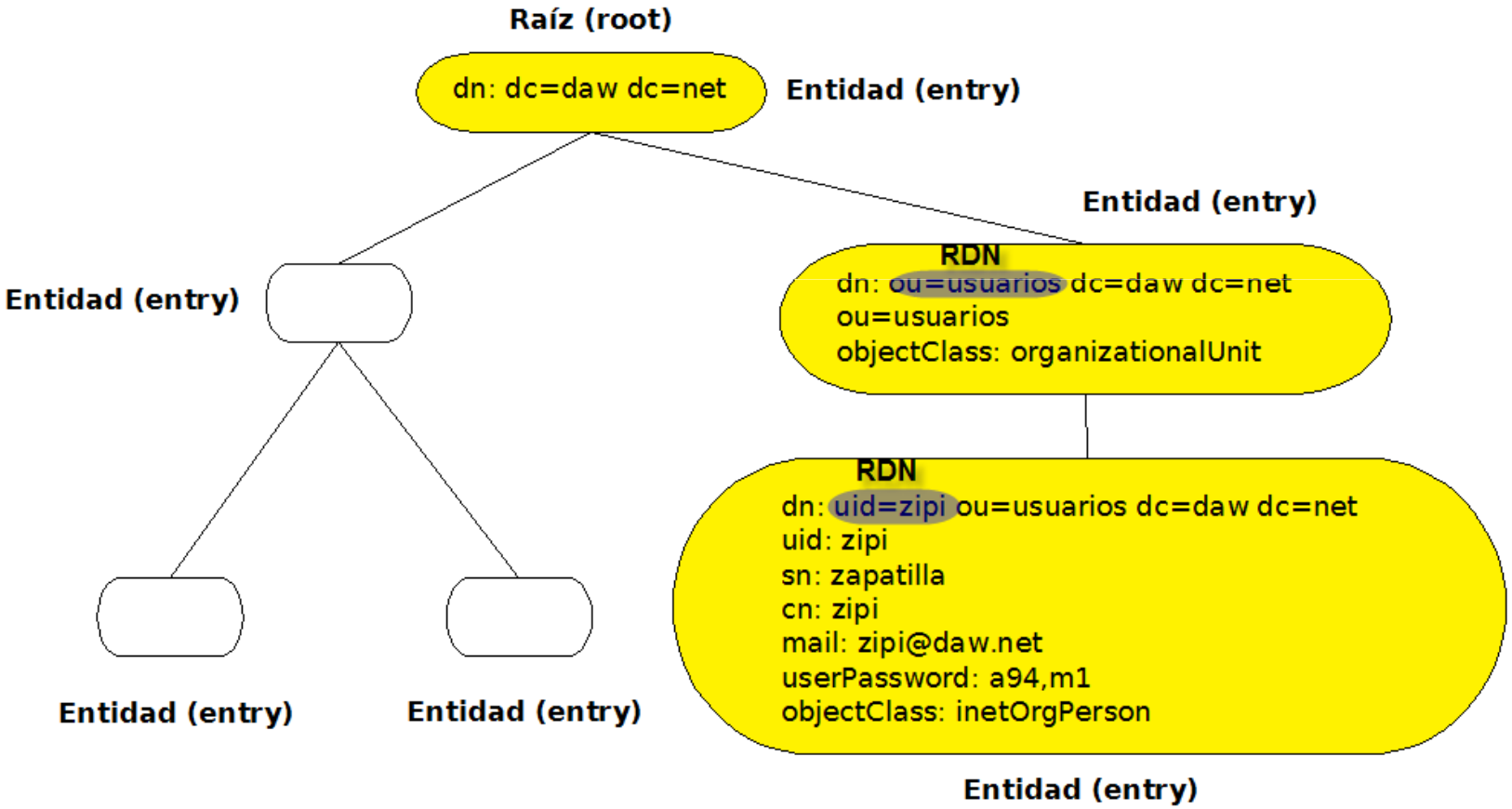
LDAP
Modelo de nombrado

- DN (*Distinguished Name*): nombre único que identifica de forma unívoca a una entrada.
- Secuencias de RDNs (*Relative Distinguished Names)* y cada RDN se corresponde con una rama del DIT partiendo de la raíz hacia la entrada dentro del directorio.



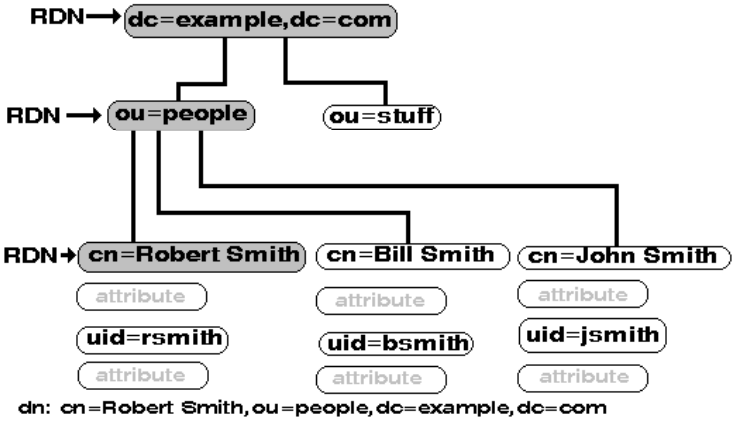
LDAP
Modelo de nombrado

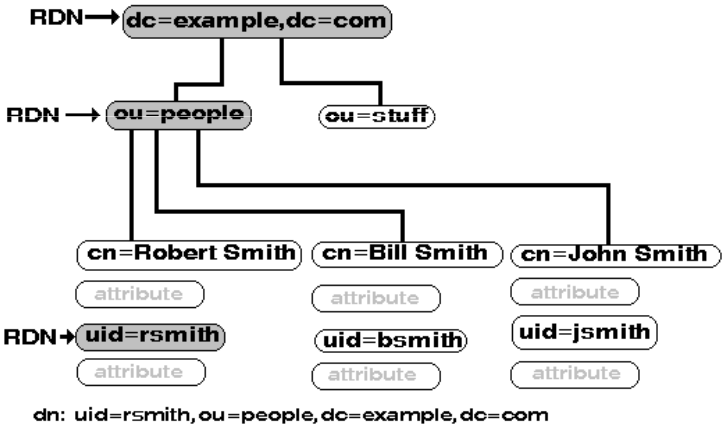
- DN = camino hasta la raíz + RDN (*relative* DN)



LDAP
Modelo de nombrado

- Se puede elegir que atributo de la entidad formara el RDN teniendo en cuenta que el DN debe ser único.

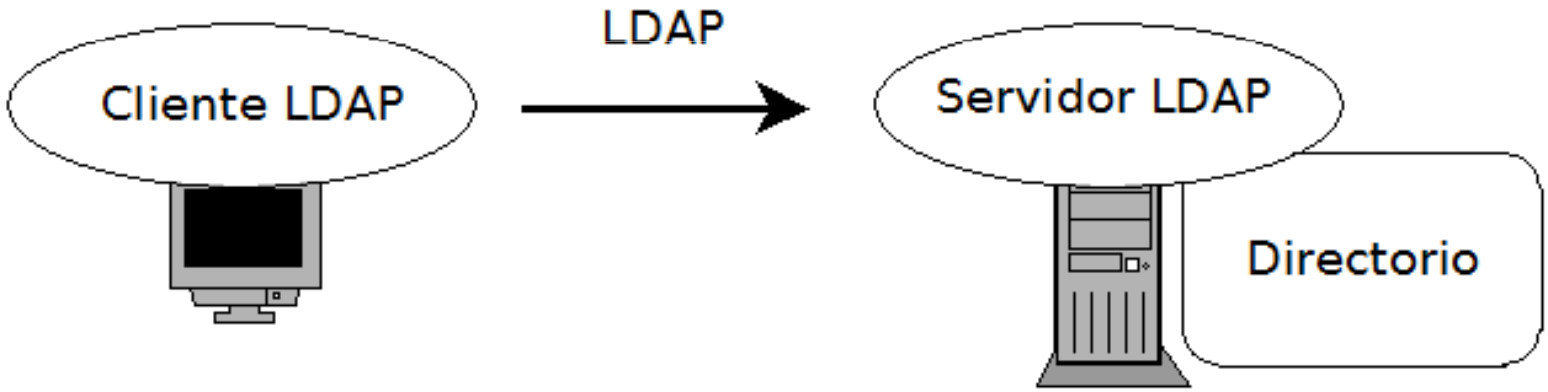




- Web (ejemplos)
  - http://www.zytrax.com/books/ldap/apa/dn-rdn.html

LDAP
Modelo de funcionamiento

- Arquitectura cliente/servidor.
  - Servidor -> Puerto 389/TCP



Práctica

- Práctica 9.1
  - Instalación de *OpenLDAP* 2.4 en *Linux.*


```
dn: dc=daw01,dc=net
objectClass: top
objectClass: dcObject
objectClass: organization
o: daw01.net
dc: daw01

dn: cn=admin,dc=daw01,dc=net
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
```

Biblografía

- http://www.zytrax.com/books/ldap/
- Introducción al Servicio de Directorio. Rafael Calzada Pradas.
- http://www.wikipedia.org
- http://httpd.apache.org
- http://tomcat.apache.org