Servicio de Directorio LDAP

Un **servicio de directorio** es un software que almacena y organiza la información sobre los usuarios de una red de ordenadores y sobre los recursos de red. A esto se le llama normalmente un **directorio**. Los administradores utilizan este servicio para gestionar el acceso a los recursos de la red. El término servicio de directorio no debería confundirse con un repositorio de ficheros de red ni con una base de datos. Se presupone que en estos casos estamos siempre hablando de los servicios basados en los estándares X.500.

Un ejemplo muy básico de un **servicio de directorio** podría ser una tabla sencilla en la que almacenamos los recursos de una red con su IP. Ya no necesitamos memorizar la IP de cada recurso, puesto que con su nombre estaríamos ya accediendo a tal recurso.

NOMBRE	IP
Router	192.168.1.1
Equipo 0001	192.168.1.10
Equipo 0002	192.168.1.23
…	…

A nivel de servidor de directorio, cada recurso es un objeto con propiedades diferentes. Según se fue incrementando la sofisticación de los mismos, se añadieron multitud de características adicionales diseñadas para organizar toda esa información, permitir el acceso a la misma, etc.

Las características principales de los **servicios de directorio son:**

- Arquitectura cliente/servidor.
- Organización jerárquica de la información
- Estructura flexible
- Optimizado para la lectura de información, no la escritura
- Distribuidos.

X.500 es un conjunto de estándares sobre servicios de directorio, desde el punto de vista de unas bases de datos de direcciones. Incluye los siguientes protocolos:

- **Protocolo de acceso al directorio (DAP):** basado en la pila de protocolos OSI.

- Protocolo de sistema de directorio **(DSP)**

- Protocolo de ocultación de información de directorio **(DISP)**

- Protocolo de gestión de enlaces operativos de directorio **(DOP)**

El protocolo **LDAP** fue creado originalmente como una versión liviana de X.500, y terminó por reemplazarlo. Definido por la ITU, ofrece las mismas funcionalidades que DAP, pero sobre la pila de protocolos TCP/IP. Actualmente, está por la versión 3, y ofrece SSL/TLS y Certificados digitales.

LDAP

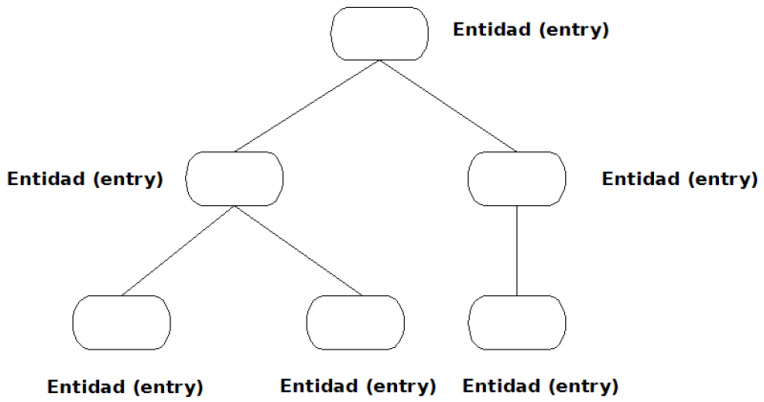
En principio, LDAP es solo un protocolo que define cómo acceder a un servicio de directorio. También define y describe cómo se representa la información en el directorio, y cómo se importa/exporta dicha información. Lo que no hace es definir cómo esa información se almacena en el directorio.

LDAP se divide en:

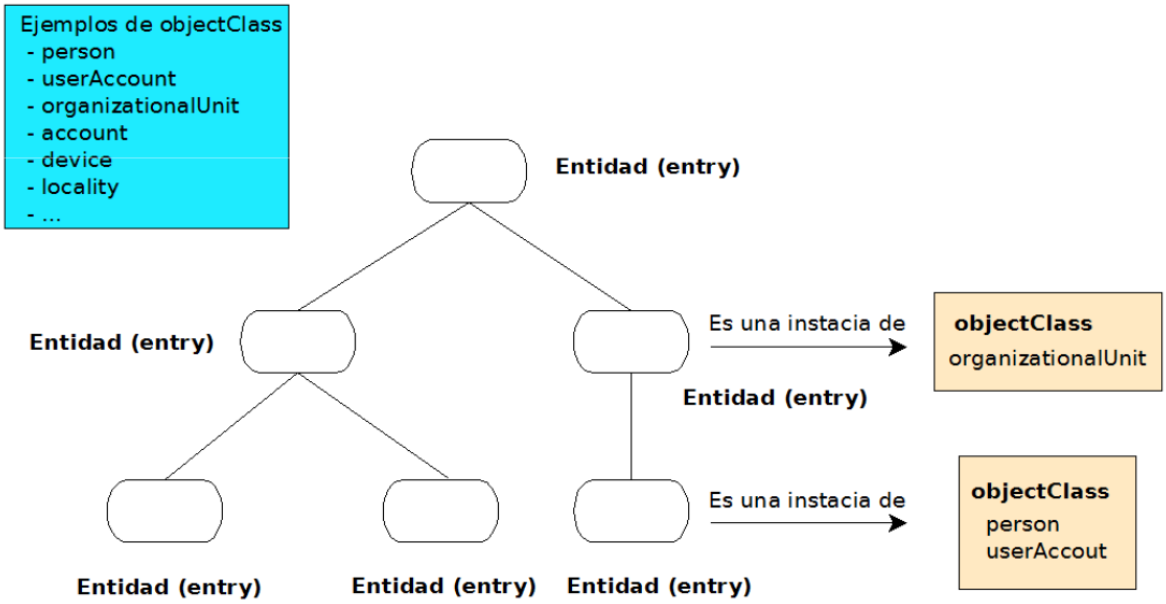
- Modelo de datos: Define la estructura de la información del directorio.
- Modelo de nombrado: Cómo se nombra y se identifica la información del directorio.
- Modelo funcional: Qué operaciones pueden realizarse sobre la información, entendiendo como tales las búsquedas, lecturas, escrituras y modificaciones.
- Modelo de seguridad: Control de acceso a los recursos del directorio.

Modelo de Datos

La información dentro de un servicio de directorio LDAP se divide en una serie de objetos llamados entradas (**entry**). Se organizan en forma de árbol, estructura que recibe el nombre de **DIT** (Data Information Tree).



Cada una de estas entidades (entry) es en realidad una instancia de una o varias clases (*objectClass*). Podemos definir tantas como queramos. Por ejemplo:



Podríamos definir una entidad como instancia de organizationalUnit y otra como persona y userAccount. A su vez, cada uno de estos *objectClass* dispone de una serie de atributos, tanto obligatorios como opcionales. Por ejemplo:

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

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

Al tratarse de clases, los *objectClass* pueden formar parte de una jerarquía y heredar los atributos de sus padres. Pueden ser de tipo:

- Estructural: Cada entidad debe pertenecer a un único *objectClass* Estructural.
- Auxiliares: Cada entidad pueden pertenecer a uno o varios *objectClass* Auxiliares.
- Abstractos: Cada entidad puede pertenecer a un único *objectClass* Abstracto.

Todo este mecanismo funciona de forma similar a la herencia de objetos. Adicionalmente, cada entidades dispone de un atributo especial que especifica todos los objectClass(es) a los que pertenece.

Finalmente, de la misma forma que utilizamos esquemas para definir la estructura de una base de datos, LDAP dispone de sus propios **esquemas** para decir toda la información de su modelo de datos. No obstante, utiliza un sistema diferente, similar a una exportación de las tablas de una BBDD:

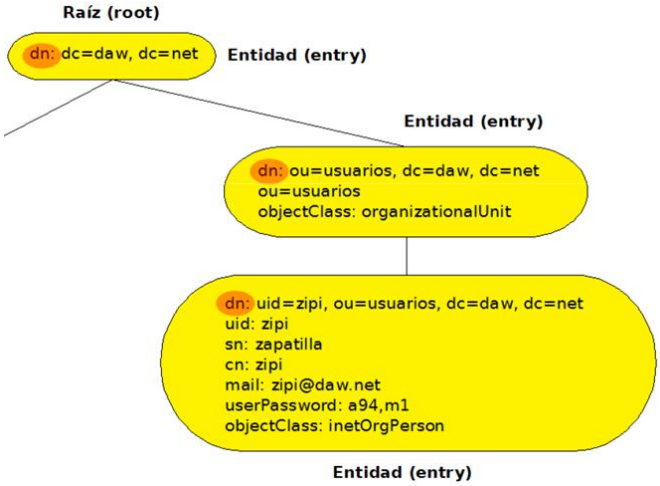
```
objectclass ( 2.5.6.6 NAME 'person' SUP top STRUCTURAL
  MUST ( sn $ cn )
  MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )

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 ) )
```

Modelo de Nombrado

Define cómo se nombra y se identifica a la información almacenada en el directorio. Las entradas se organizarán en base a su **DN** (*Distinguished Name*). El DN es nombre único que identifica de forma unívoca a una entry. Puedes considerarlo similar a la ruta de un fichero en disco, con la salvedad de que recorre el árbol de abajo a arriba recorriendo cada entry.

Cada **DN** está formado por una serie de **RDN**, que son los DN Relativos de cada entry. Así, por ejemplo, para la última entry (la de Zipi Zapatilla), su DN es



DN: uid=zipi, ou=usuarios, dc=daw

Mientras que el atributo seleccionado para una entry sea único, como en la clave primaria de una base de datos, es elegible para formar parte de la DN.

Modelo Funcional

LDAP sigue el modelo estándar de arquitectura Cliente-Servidor. Adicionalmente, LDAP ofrece las siguientes operaciones:

- Consulta: Similares en concepto a las de bases de datos. Operaciones de búsqueda y lectura de información (**search**)
- Actualización: Equivalentes a las operaciones de inserción (**add**), borrado (**delete**) y modificación (**modify**) de base de datos. Dispone de una más destinada a renombrar un DN de una entry (**rename**).
- Autenticación y control: (**bind**, **unbind**, …)