址进行了映射。采用名字服务这种类型的目录，用户不必记住某个网络资源的物理地址，只需要提供这个网络资源的名字就可以找到它。在网络上的每一个资源都被目录服务当作一个对象，关于某个网络资源的信息被作为这个对象的属性存储起来。存储到对象之内的信息可以进行访问控制以增强安全性，这样只有授权的用户才能访问到这些信息。

目录服务遵循 LDAP 和 X.500 协议。一些厂商提供了自己的目录服务产品，如微软公司的 Active Directory、Novell 公司的 eDirectory、IBM 的 Tivoli Directory、开源的 OpenLDAP 等。

现在目录服务用于管理各种大量的信息，其中包括 QoS、带宽管理策略、配置文件、电子商务信息及其他信息，在用户的身份验证、防火墙过滤及 VPN 访问方面也起着重要的安全作用。

目录服务在电子商务和企业对企业之间的关系中扮演着重要角色。目录可保存有关公司网络外部人员的重要信息，用于鉴别这些人员并定义他们对于网络资源的访问权。

6.1.2　X.500 协议简介

X.500 是国际电信联盟（ITU-T）定义的目录标准，它主要充当商业产品的一种模型。设计 X.500 的目的是使用 OSI 协议族，但是 TCP/IP 却成为了实际的网络协议，因此，如今大多数目录服务都以 X.500 为模型并设计用于在 TCP/IP 上运行。

X.500 是一个协议族，由一系列的概念和协议组成，包括：

① X.501：模型定义，定义目录服务的基本模型和概念。

② X.509：认证框架，定义如何处理目录服务中的客户和服务器认证。

③ X.511：抽象服务定义，定义 X.500 提供的功能性服务。

④ X.518：分布式操作过程定义，定义如何跨平台处理目录服务。

⑤ X.519：协议规范，定义了 X.500 协议，包括 DAP（Directory Access Protocol，目录访问协议）、DSP（Directory System Protocol，目录系统协议）、DOP（Directory Operator Protocol，目录操作绑定协议）、DISP（Directory Information Shadowing Protocol，目录信息阴影协议）。

⑥ X.520：定义属性类型要求。

⑦ X.521：定义对象类型。

⑧ X.525：定义如何在目录服务器间复制内容。

X.500 标准中定义了很多内容，包括：

① 定义信息模型，确定目录中信息的格式和字符集，如何在项中表示目录信息（定义对象类、属性等模式）。

② 定义命名空间，确定对信息进行的组织和引用，如何组织和命名项、目录信息树（DIT，Directory Information Tree）和层次命名模型。

③ 定义功能模型，确定可以在信息上执行的操作。

④ 定义认证框架，保证目录中信息的安全，以及如何实现目录中信息的授权保护（访问控制模型）。

⑤ 定义分布操作模型，确定数据如何分布和如何对分布数据执行操作，如何将全局目录树划分为管理域，以便管理。

⑥ 定义客户端与服务器之间通信的各种协议。

X.500 主要具备以下特征。

① 分散维护：运行 X.500 的每个站点只负责其本地目录部分，所以可以立即进行更新和维护操作。

② 强大的搜索性能：X.500 提供强大的搜索功能，支持用户建立的任意复杂查询。

③ 单一全局命名空间：类似于 DNS，X.500 为用户提供单一的相同命名空间。与 DNS 相比，X.500 的命名空间更灵活且易于扩展。

④ 结构化信息结构：X.500 目录中定义了信息结构，允许本地扩展。

⑤ 基于标准的目录服务：由于 X.500 可以被用于建立一个基于标准的目录，那么在某种意义上，请求应用目录信息（电子邮件、资源自动分配器、特定目录工具）的应用程序就能访问重要且有价值的信息。

X.500 虽然是一个完整的目录服务协议，但在实际应用的过程中却存在着不少障碍。由于目录访问协议 DAP 这种应用层协议是严格遵照复杂的 ISO 七层协议模型制定的，对相关层协议环境要求过多，主要运行在 UNIX 机器上，在许多小系统上，如 PC 和 Macintosh 上无法使用，因此没有多少人按照 DAP 开发应用程序，TCP/IP 协议体系的普及更使得这种协议越来越不适应需要。

由于 X.500 的实施太过复杂而受到批评。为解决这个问题，密歇根州立大学推出了一种较为简单的基于 TCP/IP 的 DAP 新版本，即轻量级目录访问协议（LDAP，Lightweight Directory Access Protocol），主要用于 Internet。LDAP 与 DAP 具有很多类似的基本功能，另外它还能用来查询私有目录和开放 X.500 目录上的数据。在过去的几年里，大多数主要的电子邮件和目录服务软件供应商都对 LDAP 表现出了极大的兴趣，LDAP 已迅速发展成为 Internet 上事实的目录协议标准。

6.1.3 LDAP 协议简介

LDAP 的目的很明确，就是要简化 X.500 目录的复杂度以降低开发成本，同时适应 Internet 的需要。LDAP 已经成为目录服务的标准，它比 X.500 DAP 协议更为简单实用，而且可以根据需要定制，因而实际应用也更为广泛。

与 X.500 协议相比，LDAP 在 4 个方面对 X.500 的 DAP 进行了简化：

① 功能方面。LDAP 提供 DAP 大多数功能的较低开销实现，去掉了 DAP 的冗余操作和很少使用的功能，简化了客户端和服务器端的实现。

② 数据表示方面。在 LDAP 中，大多数数据元素使用简单字符串表示，简化了实现和提高了效率。当然，为了提高效率，字符串包装在二进制编码的消息中。

③ 编码方面。使用 X.500 的编码规则子集对 LDAP 消息编码，从而能够简化实现。

④ 传输协议。LDAP 使用 TCP 传输协议，而不是 OSI 多层网络协议栈，实现得到简化，性能得到提升，完全去除了对 OSI 的依赖，使 LDAP 目录的部署更加简单。

X.500 采用公钥基础结构（PKI）作为主要的认证方式，而 LDAP 最初并不考虑安全问题，目前已增加了安全机制。为保证数据访问安全，可使用 LDAP 的 ACL（Access Control List，访问控制列表）来控制对数据读和写的权限。

LDAP 目前有第 2 版 LDAP v2 和第 3 版 LDAP v3 两个版本，基于 LDAP v3 的服务器可以让用户使用支持 LDAP 功能的 Web 浏览器，进行有关电子邮件用户的查询，可以查询的用户属性包括姓名、电话号码、电子邮件地址和地址信息等；系统管理员可以通过 LDAP 客户程序远程进行目录管理操作，如添加、删除和修改用户账户信息等；可以请求服务器执行扩展操作。

6.1.4　LDAP 模型简介

LDAP 模型是从 X.500 协议中继承而来的，是 LDAP 的一个组成部分，用于指导客户如何使用目录服务。LDAP 定义了 4 个模型，包括信息模型（Information Model）、命名模型（Naming Model）、功能模型（Functional Model）、安全模型（Security Model）。

1．信息模型

LDAP 信息模型用于描述 LDAP 中信息的表达方式，包含 3 部分：条目（Entries）、属性（Attributes）、值（Values）。LDAP 使用专有逻辑格式存储信息，这种模型既不是关系的，也不是完全面向对象的。简单概括为：

① LDAP 中信息逻辑上表示为条目。

② 条目包含一到多个对象类。

③ 每个对象类由多个属性组成。

④ 每个属性包含一到多个同一类型的数值。

⑤ 对象类和属性的类型定义构成了 schema。

条目是目录中最基本的信息单元，可以理解为目录树中的一个节点。LDAP 客户和服务器使用条目共享信息，条目是 LDAP 服务器的基本元素。执行搜索时服务器返回一组匹配条目，但修改时一次只能影响服务器中的一个条目。条目可以被任何支持 LDAP 的客户端创建，或通过使用服务器工具导入，也可由应用程序基于非 LDAP 数据或用户输入信息创建。

在目录中添加一个条目时，该条目必须包含一个或多个对象类（objectClass），每一个对象类规定了该条目中的必选属性和可选属性。图 6-1 展示了一个典型目录的一部分，它反映了现实世界中一个组织的管理对象。

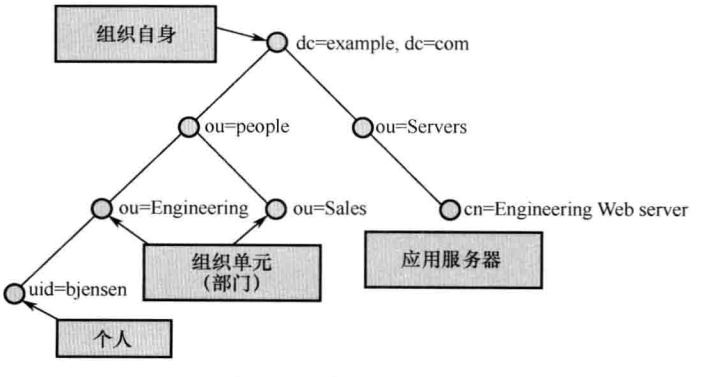

图 6-1　组织结构目录树

每一个条目都有一个 DN（distinguished name，辨别名），用于唯一标识条目在目录中的位置，本书将在命名模型中详细介绍 DN。

每个条目都是由多个属性组成的，每一个属性描述了对象的一个约束。每个属性具有一个类型和一个或多个值。该类型描述了包含在属性中的信息类型，其值中包含实际数据。例如，表 6-1 描述了一个人员条目，属性包括全称、名、姓、电话号码、电子邮件地址。

表 6-1　人员属性

属性类型	属性值
cn	张三
telephoneNumber	58046690 62300098
mail	zs@163.com

属性有与之关联的语法和匹配规则，属性语法指定可以在属性中存放的数据格式，如 INTEGER 语法允许值中只包含数字，不能包含非数字字符。

匹配规则作用有二：第一，比较值是否相等；第二，对值进行排序。

2．命名模型

LDAP 命名模型定义了如何在目录系统中组织数据以及如何从目录系统中查找数据。命名模型的灵活性可以使你很方便地以想要的方式组织数据。例如，可以把组织中所有人员放在一个容器下，所有组放在一个容器下，或按组织结构的地理分布组织目录结构。

LDAP 命名模型指定将条目按类似倒立的树结构进行规划，非常类似于 UNIX 系统的文件系统，如图 6-2 和图 6-3 所示。

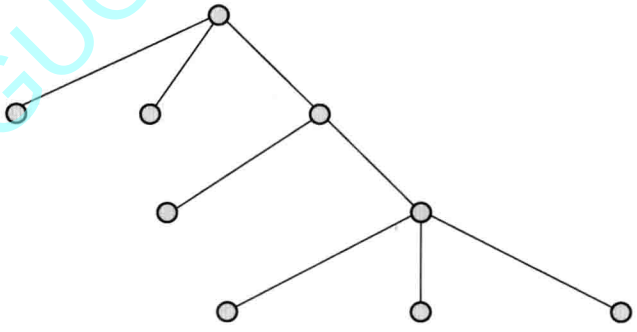

图 6-2　目录树结构

在 LDAP 目录中任何一个节点都可以包含信息，同时也可以是一个容器，也就是说任何一个 LDAP 条目都可以有子节点。图 6-4 表示了一个典型的目录结构，在目录树中，条目 ou=People，dc=example，dc=com 和条目 ou=Devices，dc=example，dc=com 都既包含属性又包含子节点。

通过命名模型，可以给出目录中任何条目的唯一名称，从而可以毫无歧义地引用任何一个条目。在 LDAP 中使用 DN 来引用条目。

在目录中，按目录树从下到上对条目进行命名，如图 6-4 中的灰色条目的 DN 名称为 uid=bjensen，ou=people，dc=example，dc=com。因为这种树形结构决定了从根节点到其他

任何一个节点的路径是唯一的，所以说每一个条目的 DN 是唯一的。

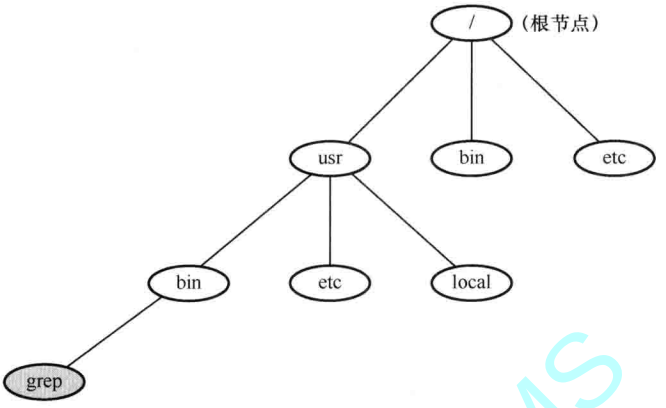

图 6-3　UNIX 文件系统

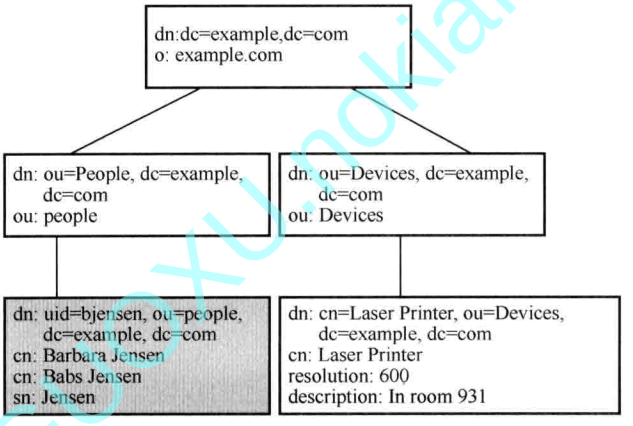

图 6-4　典型目录结构

在 DN 中最左边的内容称为相对辨别名（RDN，Relative Distinguished Name）。如 ou=People，dc=example，dc=com 的 RDN 为 ou=People。对于共享同一个父节点的所有节点的 RDN 必须是唯一的。如果不属于同一个父节点，则节点的 RDN 可以相同。

当特殊字符出现在 DN 中时，必须进行转义，如表 6-2 所示。

表 6-2　特殊字符转义表

字符	数值	转义序列	字符	数值	转义序列
在 DN 或 RDN 开始或结尾的空格	32	\空格	反斜线（\）	92	\\
在 DN 或 RDN 开始的#	35	\#	小于符（<）	60	\<
逗号（, ）	44	\,	大于符（>）	62	\>
加号（+）	43	\+	分号（;）	59	\;
双引号（"）	34	\"			

3．功能模型

LDAP 功能模型描述了 LDAP 协议可以采用的相关操作，以访问存储在目录树中的数