**Network Account Databases**  
Many networks employ network account databases, such as the Lightweight Directory  
Access Protocol (LDAP), Kerberos realms, and Active Directory (AD) domains. These systems move account database management onto a single centralized computer (often with  
one or more backup systems). This approach’s advantage is that users and administrators  
need not deal with maintaining accounts independently on multiple computers. A single  
account database can handle accounts on dozens (or even hundreds or thousands) of different computers, greatly simplifying day-to-day administrative tasks and users’ lives.  
Linux can participate in these systems. In fact, some distributions provide options to  
enable such support at OS installation time. Typically, you must know the name or IP  
address of the server that hosts the network account database, and you must know what  
protocol that server uses. You may also need a password or some other protocol-specific

information, and the server may need to be configured to accept accesses from the Linux  
system you’re configuring.  
Using such a system with Linux means that most user accounts won’t appear in /etc/  
passwd and /etc/shadow. Groups may not appear in /etc/group. However, these files  
will still hold information on local system accounts and groups.  
Activating use of such network account databases after installing Linux is a complex  
topic. It involves installing appropriate software and modifying various configuration  
files. Such systems often alter the behavior of tools such as passwd and usermod in subtle  
or not-so-subtle ways. If you want to use such a system, you’ll have to consult documentation specific to the service you intend to use.