## Trees

A *tree* is a set of Active Directory names that share a namespace. The domains `nimbusbroom.com`, `accounting.nimbusbroom.com`, `manufacturing.nimbusbroom.com`, and `sales.nimbusbroom.com` make up a tree that's derived from a common root domain, `nimbusbroom.com`.

The domains that make up a tree are related to one another through *transitive trusts.* In a transitive trust, if DomainA trusts DomainB and DomainB trusts DomainC, DomainA automatically trusts DomainC.


TIP

Note that a single domain all by itself is still considered to be a tree.

## Forests

As its name suggests, a *forest* is a collection of trees. In other words, a forest is a collection of one or more domain trees that do *not* share a common parent domain. Every domain must belong to a forest, so even if your organization has just one domain, you'll also have one forest.

But suppose your company (Nimbus Brooms) acquires Tracorum Technical Enterprises, which already has its own root domain named `tracorumtech.com`, with several subdomains of its own. You can create a forest from these two domain trees so that the domains can trust each other.

# Understanding Windows User Accounts

Now that we've reviewed the basic organizational structure of Active Directory, let's look at how users accounts are created and managed. As you might guess, user accounts are among the basic tools for managing a Windows server. As a network administrator, you'll spend a large percentage of your time dealing with user accounts — creating new ones, deleting expired ones, resetting passwords for forgetful users, granting new access rights, and so on.

The following sections describe some of the pertinent characteristics of user accounts.

## Local accounts versus domain accounts

A *local account* is a user account stored on a particular computer, applicable to that computer only. Typically, each computer on your network has a local account for each person who uses that computer.