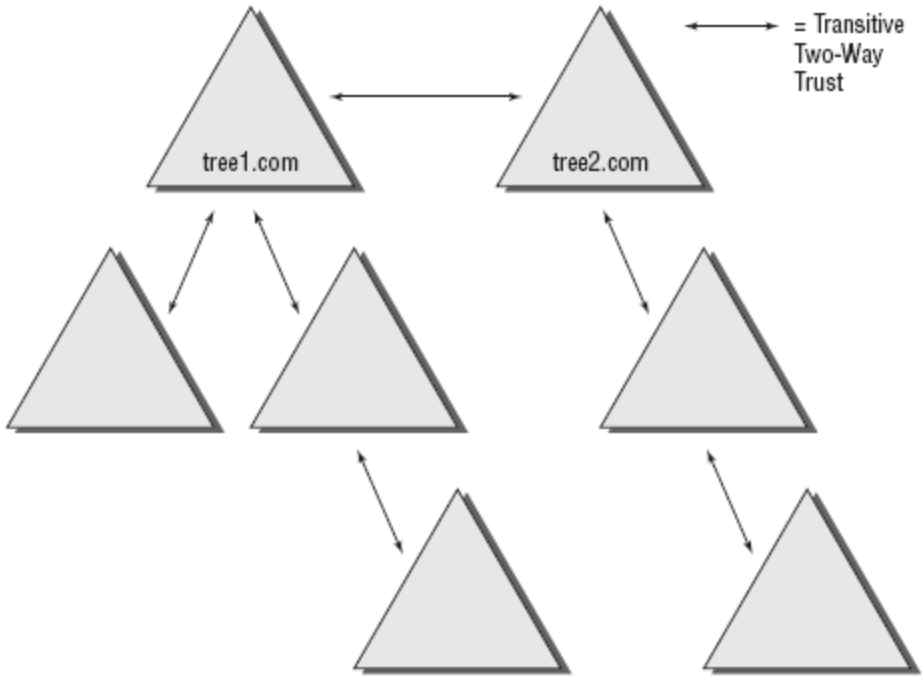
Managing Trusts

Trust relationships make it easier to share security information and network resources between domains. As was already mentioned, standard transitive two-way trusts are automatically created between the domains in a tree and between each of the trees in a forest. Figure 4.4 shows an example of the default trust relationships in an Active Directory forest.

FIGURE 4.4 Default trusts in an Active Directory forest



When configuring trusts, here are two main characteristics you need to consider:

Transitive trusts By default, Active Directory trusts are *transitive trusts*. The simplest way to understand transitive relationships is through an example like the following: If Domain A trusts Domain B and Domain B trusts Domain C, then Domain A implicitly trusts Domain C. If you need to apply a tighter level of security, trusts can be configured as intransitive.

One-way vs. two-way Trusts can be configured as one-way or two-way relationships. The default operation is to create *two-way trusts* or *bidirectional trusts*. This makes it easier to manage trust relationships by reducing the trusts you must create. In some cases, however, you might decide against two-way trusts. In one-way relationships, the trusting domain allows resources to be shared with the trusted domain, but not the other way around.

When domains are added together to form trees and forests, an automatic transitive two-way trust is created between them. Although the default trust relationships work well for most organizations, there are some reasons why you might want to manage trusts manually:

- You may want to remove trusts between domains if you are absolutely sure that you do not want resources to be shared between domains.
- Because of security concerns, you may need to keep resources isolated.

In addition to the default trust types, you can also configure the following types of special trusts:

External trusts You use *external trusts* to provide access to resources on a Windows NT 4 domain or forest that cannot use a forest trust. Windows NT 4 domains cannot benefit from the other trust types that are used in Windows Server 2008, so in some cases, external trusts could be your only option. External trusts are always nontransitive, but they can be established in a one-way or two-way configuration.

> **Default SID filtering on external trusts** When you set up an external trust, remember that it is possible for hackers to compromise a domain controller in a trusted domain. If this trust is compromised, a hacker can use the security identifier (SID) history attribute to associate SIDs with new user accounts, granting themselves unauthorized rights (this is called an elevation-of-privileges attack). To help prevent this type of attack, Windows Server 2008 automatically enables SID filter quarantining on all external trusts. SID filtering allows the domain controllers in the trusting domain (the domain with the resources) to remove all SID history attributes that are not members of the trusted domain.

Realm trusts *Realm trusts* are similar to external trusts. You use them to connect to a non-Windows domain that uses Kerberos authentication. Realm trusts can be transitive or nontransitive, one-way or two-way.

Cross-forest trusts *Cross-forest trusts* are used to share resources between forests. They have been used since Windows Server 2000 domains and cannot be intransitive, but you can establish them in a one-way or a two-way configuration. Authentication requests in either forest can reach the other forest in a two-way cross-forest trust.

> **Selective authentication vs. forest-wide authentication** Forest-wide authentication on a forest trust means that users of the trusted forest can access all the resources of the trusting forest. Selective authentication means that users cannot authenticate to a domain controller or resource server in the trusting forest unless they are explicitly allowed to do so. Exercise 4.4 will show you the steps to change forest-wide authentication to selective authentication.

Shortcut trusts In some cases, you may actually want to create direct trusts between two domains that implicitly trust each other. Such a trust is sometimes referred to as a *shortcut trust* and can improve the speed at which resources are accessed across many different domains.

Explaining outgoing Trusts

A one-way, outgoing, forest trust allows resources in your Windows Server 2008 forest or Windows Server 2003 forest (the forest that you are logged on to at the time that you run the New Trust Wizard) to be accessed by users in another Windows Server 2008 forest or Windows Server 2003 forest. For example, if you are the administrator of the wingtiptoys.com forest and resources in that forest need to be accessed by users in the tailspintoys.com forest, you can use this procedure to establish one side of the relationship so that users in the tailspintoys.com forest can access resources in any of the domains that make up the wingtiptoys.com forest.

Explaining incoming Trusts

A one-way, incoming, forest trust allows users in your Windows Server 2008 forest or Windows Server 2003 forest (the forest that you are logged on to at the time that you run the New Trust Wizard) to access resources in another Windows Server 2008 forest or Windows Server 2003 forest. For example, if you are the administrator of the wingtiptoys.com forest and users in that forest need to access resources in the tailspintoys.com forest, you can use this procedure to establish one side of the relationship so that users in your forest can access resources in any of the domains that make up the tailspintoys.com forest.