# Understanding Trust Relationships

In a trust relationship, the two domains are referred to as the trusting domain and the trusted domain. The trusted domain is the domain where the trust relationship is created. The trusting domain is the other domain specified in the trust, that is, the one wherein network resources can to be accessed. The trusting domain in this case recognizes the logon authentications of the trusted domain. The NT LanMan Challenge Response supports the logon trust relationship. This allows pass-through authentication of users from the trusted domain. One of the shortfalls of Windows NT trust relationships is that trusts between domains were one way and non-transitive. This meant that the defined trust relationship ended with the two domains between which the particular trust was created. The rights implicit in the trust relationship also flowed only in one direction. Because of this, defining and managing trust relationships in the Windows NT domain structure was a cumbersome and labor intensive task. The Windows NT domain worked well in small enterprises where one domain typically existed in the enterprise. In those larger enterprises that have multiple domains, Administrators have to define trust relationships between the domains in order for a user in one domain to access resources in another domain.

The characteristics of Windows Server 2003 trusts are outlined below:

- Trusts can be non-transitive or transitive:
    - Transitive trusts: With transitive trusts, trust is applicable for each trusted domain. What this means is where Domain1 trusts Domain2, and Domain2 trusts Domain3, Domain1 would also trust Domain3.
    - Non-transitive trust: The defined trust relationship ends with the two domains between which the particular trust is created.
- Trusts can be one way or two way:
    - One way trusts: Based on the direction of the trust, one way trust can further be broken into either incoming trust or outgoing trusts. One way trust can be transitive or non-transitive:
        - Incoming Trust: With incoming trust, the trust is created in the trusted domain and users in the trusted domain are able to access network resources in the trusting domain or other domain. Users in the other domain cannot however access network resources in the trusted domain.
        - Outgoing Trust: In this case, users in the other domain can access network resources in the initiating domain. Users in the initiating domain are not able to access any resources in the other domain.
    - Two way trusts: A two way trust relationship means that where Domain1 trusts Domain2, then Domain2 trusts Domain1. The trust basically works both ways and users in each domain are able to access network resources in either one of the domains. A two way, transitive trust relationship is the trust that exists between parent domains and child domains in a domain tree. In two way transitive trust, where Domain1 trusts Domain2 and Domain2 trusts Domain3, then Domain1 would trust Domain3 and Domain3 would trust Domain1.Two way transitive trust is the default trust relationship between domains in a tree. It is automatically created and exists between top level domains in a forest.
- Trusts can be implicit or explicit trusts:
    - Implicit: Automatically created trust relationships are called implicit trust. An example of implicit trust is the two way transitive trust relationship that Active Directory creates between a parent and child domains.

- Explicit: Manually created trust relationships are referred to as explicit trust.

## Types of Active Directory Trust Relationships

The types of trust relationships that can be created and configured for Active Directory domains are discussed in this section. As an Administrator for Active Directory Windows Server 2003 domains, it is important to understand the different types of trusts that are supported in Windows Server 2003 and to know which trust relationship to create for the different network resource access requirements that exist within the organization.

- **Tree-root trust**: Tree root trust is automatically/implicitly created when a new tree root domain is added to a forest. The trust relationship exists between two root domains within the same forest. For instance, if there is an existing forest root domain, and a new tree root domain is added to the same forest, tree root trust is formed between the new tree root domain and the existing forest root domain. Tree root trust is transitive and two way.
- **Parent-child trust**: Parent-child trust is implicitly established when new child domains are added to a domain tree. Parent-child trust is a two-way, transitive trust relationship. Active Directory automatically creates a trust relationship between the new child domain and the domain directly above it in the domain namespace hierarchy. What this means is that the trust relationship exists between those domains that have a common contiguous DNS namespace and who are part of the same forest. Parent-child trust enables child domain authentication requests to be passed through the parent domain for authentication. In addition, when a new domain is added to the tree, trust relationships are created with each domain in the tree. This means that network resources in the tree's individual domains can be accessed by all other domains in the tree.
- **Shortcut trust**: An administrator explicitly creates a shortcut trust and is either a one way transitive trust or two way transitive trust. Shortcut trust is usually created when users want to speed up or enhance authentication performance between two domains in different trees but within the same forest. One way shortcut trust should be created when users in Domain1 need to access Active Directory objects in Domain2 but users in Domain2 do not need to access objects in Domain1. Two way shortcut trust should be created when users in each domain need to access objects in each other's domain.
- **Realm trust**: An administrator explicitly creates realm trust and it can be defined as either a transitive or non-transitive trust. It can also either be a one way or two way trust. Realm trust enables users to create a trust relationship between a Windows Server 2003 Active Directory domain and a non-Windows Kerberos version 5 realm. Realm trust therefore facilitates interoperability between a Windows Server 2003 domain and a realm used in Kerberos version 5 implementations.
- **External trust**: An administrator explicitly defines the external trust to enable trust between domains that are located in different forests and to create trust between an Active Directory domain and a down-level Windows NT 4 domain. External trust is always non-transitive but can be either one-way trusts or two-way trusts. External trust is usually only created in Windows Server 2003 Active Directory environments when users need to access network resources in a domain that resides in a different forest and forest trust cannot be created between the two domains. When external trust is created between an Active Directory domain and a down-level Windows NT 4 domain, it is a one-way, non-transitive trust relationship.

- **Forest trust**: An Administrator explicitly created Forest trust to enable trust between two Active Directory forests. Forest trust is transitive in nature and can either be one-way or two-way. Forest trust is only available in Windows Server 2003. Before users can create forest trust between two forests, each domain in the particular forest and each forest has to be raised to and run at the Windows Server 2003 functional level. Because forest trust is created between two root domains of two forests, it can create two way trusts with each domain within the two forests. This basically means that users would be able to access Active Directory objects between all domains encompassed by the particular forest trust relationship.