

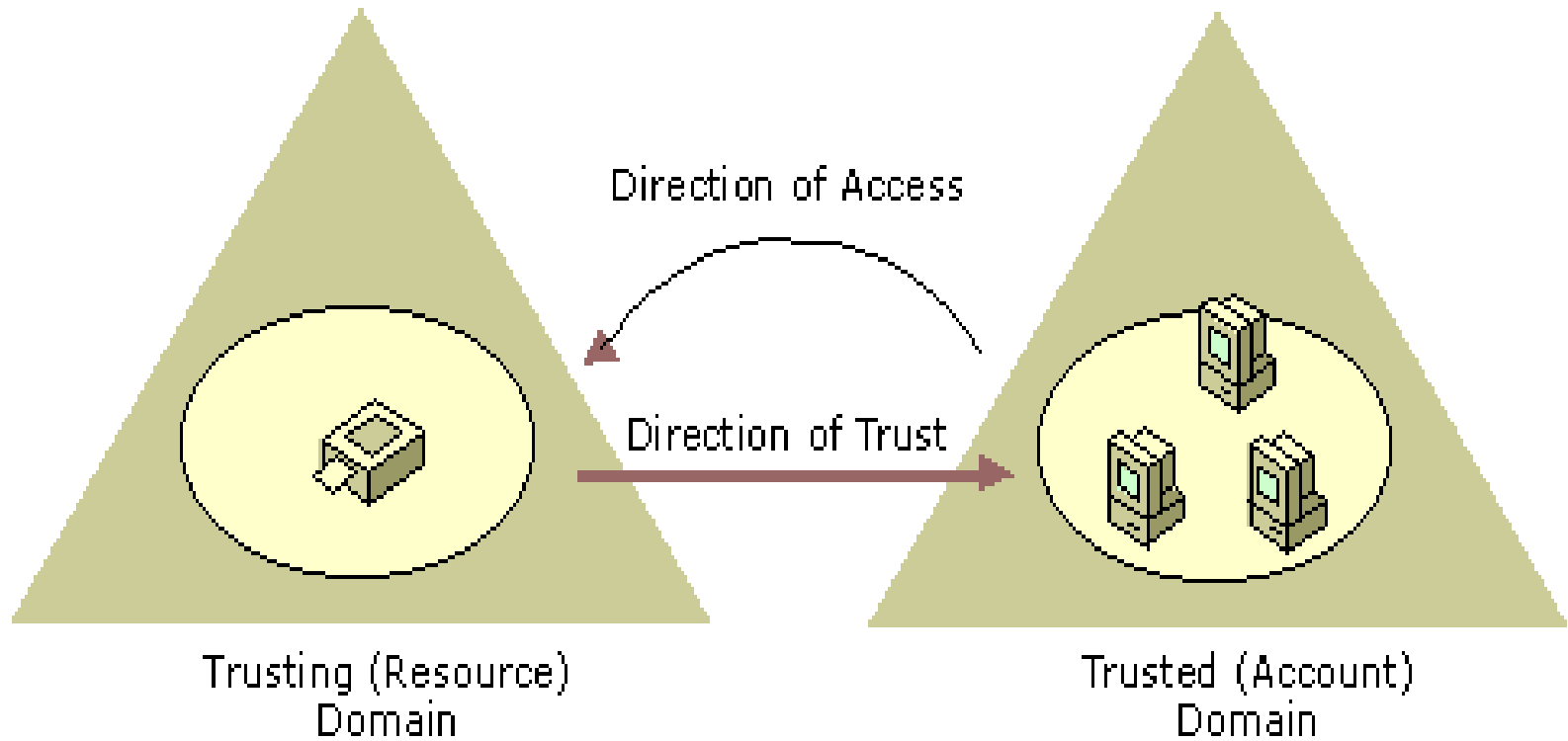
# Determining Trust Relationships

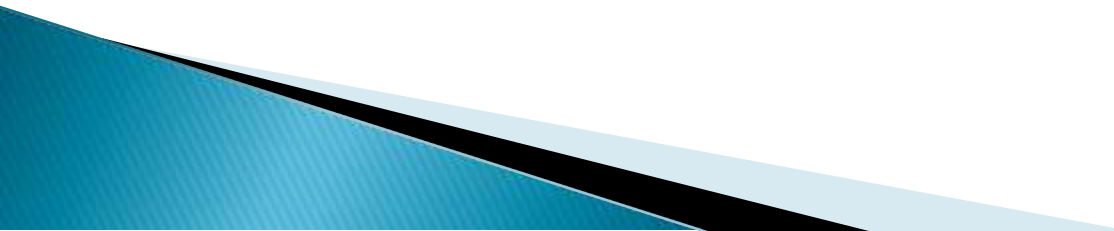
- ▶ Trust relationships are logical connections that combine two or more domains into one administrative unit. Trust relationships allow permissions to be associated and passed from one domain to another.
- ▶ With Active Directory Domains and Trusts, an administrator can establish relationships between domains that will allow users in one domain to access the resources in another

# Understanding domain trusts

- ▶ A domain trust is a relationship established between domains that enables users in one domain to be authenticated by a domain controller in the other domain. The authentication requests follow a *trust path*.
- ▶ ***Trust path***

Before a user can access a resource in another domain, Windows security must determine whether the **trusting domain** (the domain containing the resource the user is trying to access) has a trust relationship with the trusted domain (the user's logon domain).
- ▶ To determine this, the Windows security system computes the trust path between a domain controller in the trusting domain and a domain controller in the trusted domain.



- ▶ All domain trust relationships have only two domains in the relationship: the trusting domain and the trusted domain. A domain trust relationship is characterized by whether it is:
    - ▶ Two-way
    - ▶ One-way
    - ▶ Transitive
    - ▶ Nontransitive
- 

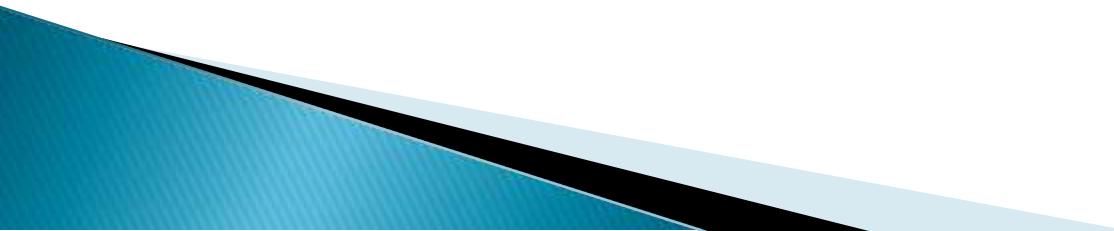
## ▶ *One-way trust*

A one-way trust is a single trust relationship, where Domain A trusts Domain B. All one-way relationships are nontransitive and all nontransitive trusts are one-way.

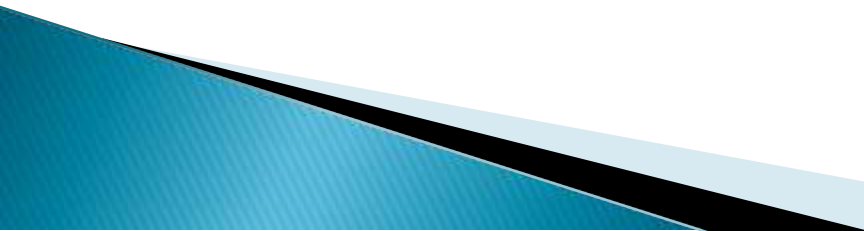
Authentication requests can only be passed from the trusting domain to the trusted domain. This means that if Domain A has a one-way trust with Domain B and Domain B has a one-way trust with Domain C, Domain A does not have a trust relationship with Domain C.

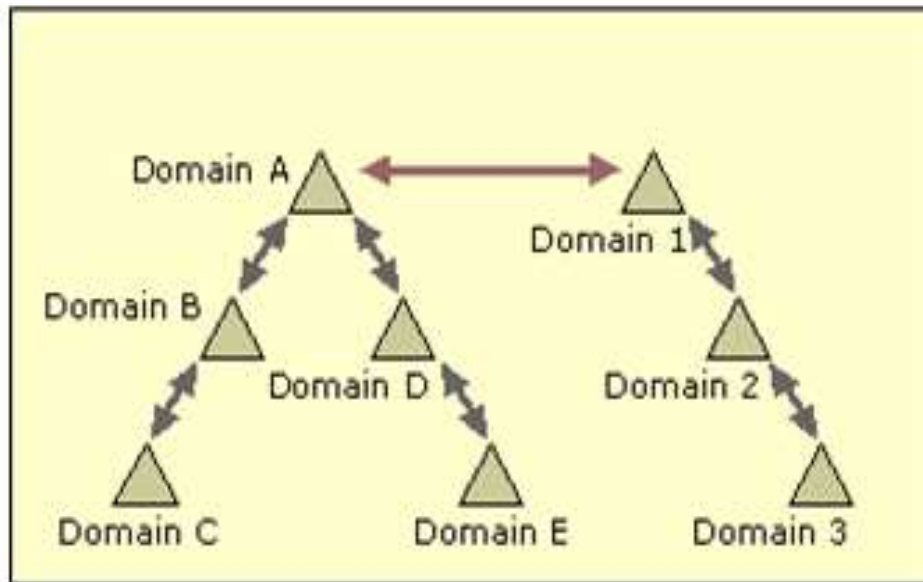
▶ ***Two-way trust***

All domain trusts in a Windows forest are two-way transitive trusts.

- ▶ When a new child domain is created, a two-way transitive trust is automatically created between the new child domain and the parent domain. In a two-way trust, Domain A trusts Domain B and Domain B trusts Domain A. This means that authentication requests can be passed between the two domains in both directions.
  - ▶ To create a nontransitive two-way trust, you must create two one-way trusts between the domains involved.
- 

## *Transitive trust*

- ▶ All domain trusts in a Windows forest are transitive. Transitive trusts are always two-way: Both domains in the relationship trust each other.
  - ▶ Transitive trust relationships flow upward through the domain tree as it is formed
  - ▶ Transitive trust relationships flow through all domains in the forest. Authentication requests follow these trust paths, so accounts from any domain in the forest can be authenticated at any other domain in the forest. With a single logon process, those accounts having the proper permissions can potentially access resources on any domain in the forest.
- 



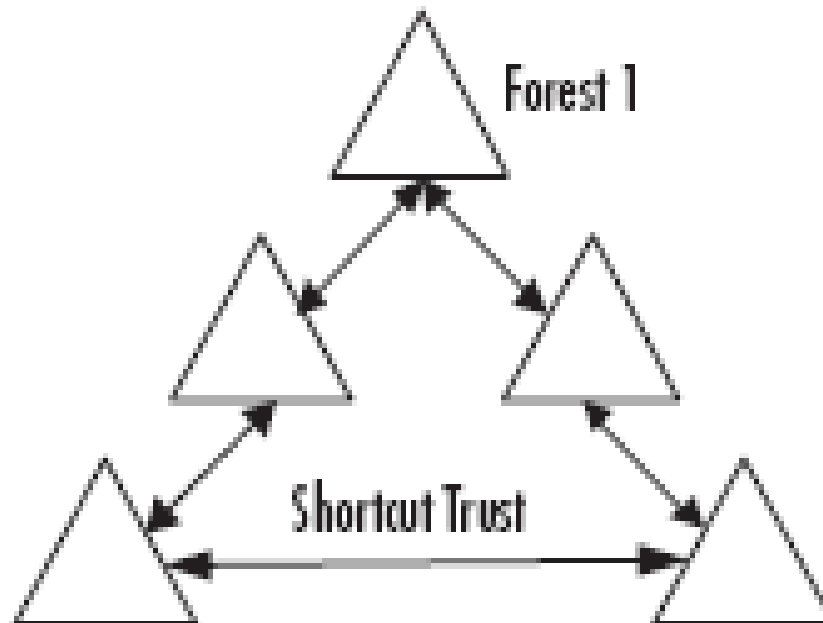
Because Domain 1 has a transitive trust relationship with Domain 2 and Domain 2 has a transitive trust relationship with Domain 3, users in Domain 3 (when granted the proper permissions) can access resources in Domain 1. Because Domain 1 has a transitive trust relationship with Domain A, and the other domains in Domain A's domain tree have transitive trust relationships with Domain A, users in Domain B (when granted the proper permissions) can access resources



- ▶ You can also explicitly (manually) create transitive trusts between Windows domains in the same domain tree or forest. These shortcut trust relations can be used to shorten the trust path in large and complex domain trees or forests.
- ▶ **Nontransitive trust**
  - A nontransitive trust is bounded by the two domains in the trust relationship and does not flow to any other domains in the forest.
- ▶ Nontransitive trusts are one-way by default

## ▶ Shortcut Trust

- ▶ Shortcut trusts are transitive in nature and can either be one-way or two-way. These trusts are used when user accounts in one domain need regular access to the resources in another domain.
- ▶ Established when the users in one domain need access to resources in the other domain, but those in the second domain do not need access to resources in the first domain.

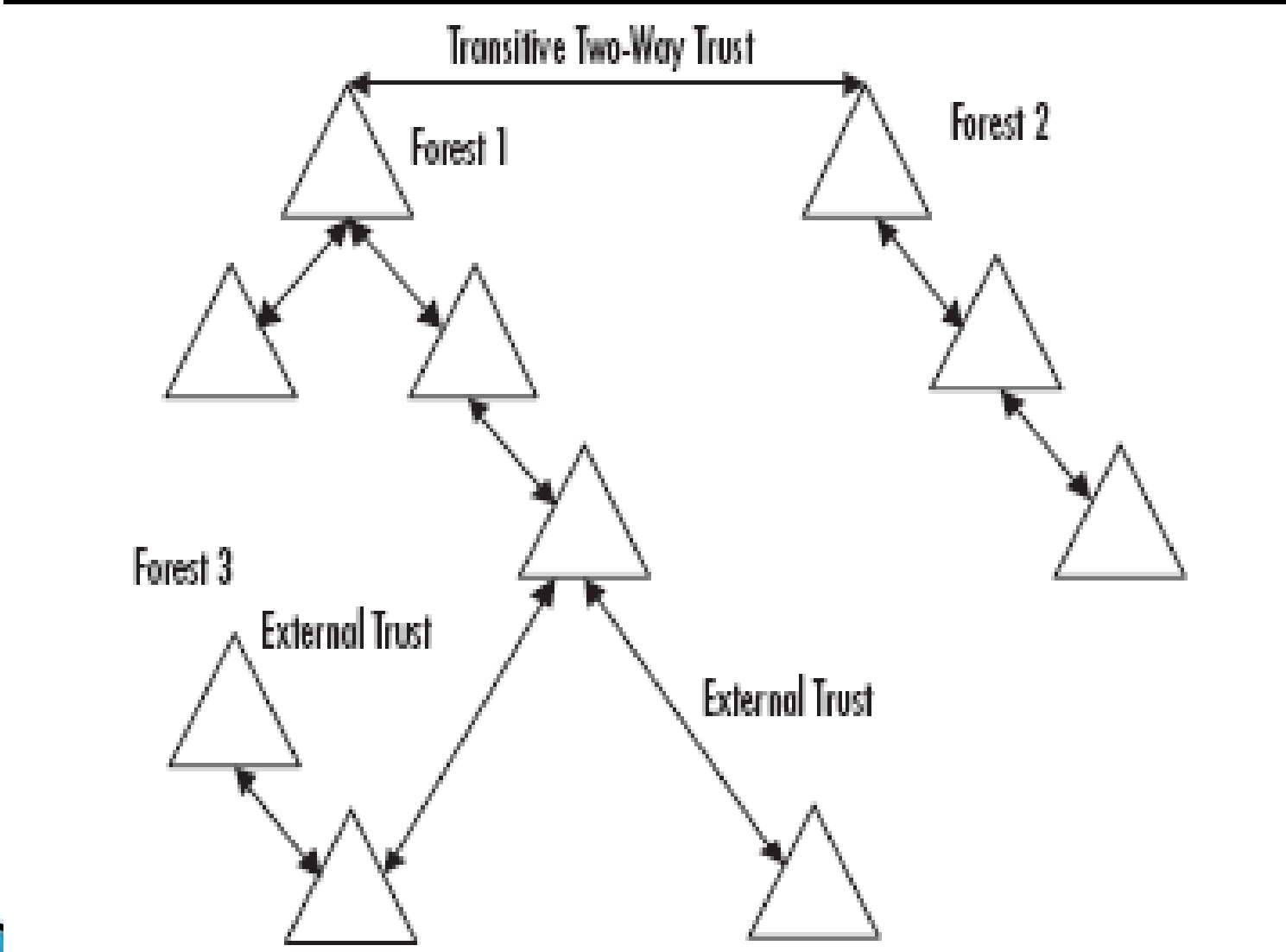


## ▶ Realm Trust

- ▶ Realm trusts are explicit trusts that are created to join a Windows Server 2003 domain to a non-Windows .This allows you the flexibility of creating a trust for your non-Windows networks to interoperate with the security services based on other Kerberos v5 implementations, such as with UNIX.

## ▶ External Trust

- ▶ An external trust is used when you need to create a trust between domains outside of your forest. These trusts can be one- or two-way trusts. They are always non-transitive in nature
- ▶ 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 new to Windows Server 2003, 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.



## ▶ Forest Trust

A forest trust can only be created between the root domains in two forests. Both forests must be Windows Server 2003 forests. These trusts can be one- or two-way trusts. They are considered transitive trusts because the child domains inside the forest can authenticate themselves across the forest to access resources in the other forest.

# Types of Trusts

