12.4.5 Active Directory Facts

Active Directory is a centralized database that contains user account and security information. In a workgroup environment, authentication, security, and management all take place on each individual computer, with each device independently storing information about users and configuration settings. Using Active Directory, all computers share the same central authentication and configuration database.

An Active Directory implementation uses the following components:

Component	Description
Trees and Forests	Multiple domains are grouped together in the following relationship: ▪ A *tree* is a group of related domains that share the same contiguous DNS namespace. ▪ A *forest* is a collection of related domain trees. The forest establishes the relationship between trees that have different DNS name spaces.

Domain	A *domain* is an administratively-defined collection of network resources that share a common directory database and security policies. The domain is the basic administrative unit of an Active Directory structure.
	▪ Database information is replicated (shared or copied) within a domain.
	▪ Security settings are not shared between domains.
	▪ Each domain maintains its own set of relationships with other domains.
	▪ Domains are identified using DNS names.
	  ▪ The common name is the domain name itself.
	  ▪ The distinguished name includes the DNS context or additional portions of the name.
	Depending on the network structure and requirements, the entire network might be represented by a single domain with millions of objects, or the network might require multiple domains.

Organizational Unit (OU)	An *organizational unit* is like a folder that subdivides and organizes network resources within a domain. An organizational unit: ▪ Is a container object ▪ Can contain other OUs or any type of leaf object (e.g., users, computers, and printers) ▪ Can be used to logically organize network resources ▪ Simplifies security administration.
Built-in Containers	Like OUs, generic built-in containers are used to organize Active Directory objects. However, built-in container objects have several differences: ▪ They are created by default. ▪ They cannot be created, moved, renamed, or deleted. ▪ They have very few editable properties.
Objects	Within Active Directory, each resource is identified as an *object*. Common objects include: ▪ Users ▪ Groups ▪ Computers You should know the following about objects: ▪ Each object contains *attributes* (i.e., information about the object, such as a user's name, phone number, and email address) which are used for locating and securing resources. ▪ Active Directory uses DNS for locating and naming objects. ▪ Container objects hold other objects, either other containers or leaf objects.
Domain Controller	A *domain controller* is a Windows server that holds a copy of the Active Directory database. ▪ A domain controller is a member of only one domain. ▪ A domain can contain multiple domain controllers. Each domain controller holds a copy of the Active Directory database. ▪ Any domain controller can make changes to the Active Directory database. ▪ *Replication* is the process of copying changes made to the Active Directory database between all of the domain controllers in the domain.

The Active Directory database resides in a file, called Ntds.dit, on the domain controller. This file stores all Active Directory data.