6.5.4 Active Directory Facts

This lesson covers the following topics:

- Active Directory
- Active Directory components

Active Directory

Active Directory is a centralized database that contains user account and security information. In a workgroup, security and management are decentralized. They take place on each individual computer; each computer holds its own information about users and resources. With Active Directory, all computers share the same central database on a remote computer called a domain controller.

Active Directory is a hierarchical database. Hierarchical directory databases have the following advantages over a flat file database structure:

Advantage	Description
Organization	Hierarchical databases let you sort and organize your user accounts by location, function, and department.
Replication	The Active Directory database can be replicated to other systems. This eliminates the need to manually recreate user accounts on every system to which a user may need to access.
Delegation	Delegation allows you to assign users to manage portions of the Active Directory database without giving all users rights to the entire database. For example, you can assign an administrator to manage the sales department in North America and enable this administrator to create user accounts, remove user accounts, and change passwords. However, this sales administrator won't be allowed to access the accounting or development departments. As another example, you can allow an administrator to manage all departments in Europe, but none in North American or Asia.
Scalability	A hierarchical database lets you grow the Active Directory to meet the needs of your environment.

Active Directory Components

Active Directory organizes network resources and simplifies management using the following components:

Component	Description
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. 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.
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

	▪ A tree is a group of related domains that share the same contiguous DNS namespaces. ▪ A forest is the highest level of the organization hierarchy and is a collection of related domain trees. The forest establishes the relationship between trees that have different DNS namespaces.
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 hold other organizational units ▪ Can hold objects such as users and computers ▪ Can be used to logically organize network resources ▪ Simplifies security administration
Generic container	Like OUs, generic containers are used to organize Active Directory objects. Generic container objects: ▪ Are created by default ▪ Cannot be moved, renamed, or deleted ▪ Have very few properties you can edit
Object	Within Active Directory, each resource is identified as an object. Common objects include: ▪ Users ▪ Groups ▪ Computers ▪ Shared folders Each object contains additional information about the shared resource that can be used for locating and securing resources. Groups are composed of other directory objects that have a common level of access. The schema identifies the object classes (the type of objects) that exist in the tree and the attributes (properties) of the objects. In Active Directory, each user is assigned a Security Account Manager (SAM) account name; therefore, each user name must be unique.
Domain controller	A domain controller is a server that holds a copy of the Active Directory database that can be written to. Replication is the process of copying changes to Active Directory between the domain controllers. In contrast, member servers are servers in the domain that do not have the Active Directory database.