Diploma in Infocomm & Security

IT2654: Systems Administration & Security

TOPIC 1: INTRODUCTION TO WINDOWS SERVER

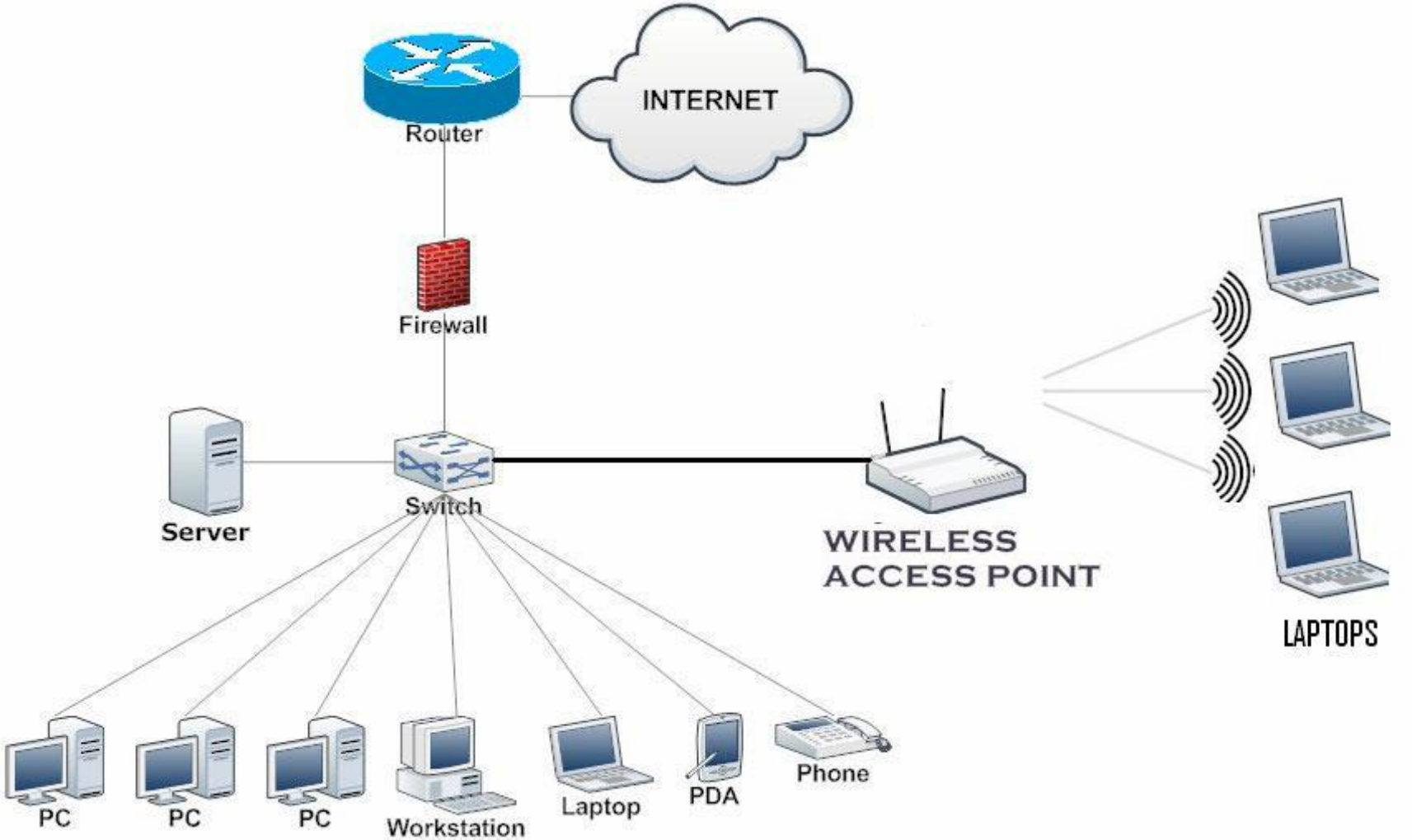
Objectives

- Server Network Administration goals
- Differentiate between the different editions of Windows Server
- Explain Windows Server network models and server roles
- Explain Windows Server Active Directory concepts

Windows Server Network Administration Goals

- To ensure that network resources such as files, folders, and printers are available to users
- To secure the network so that available resources are only accessible to users who have been granted the proper permissions

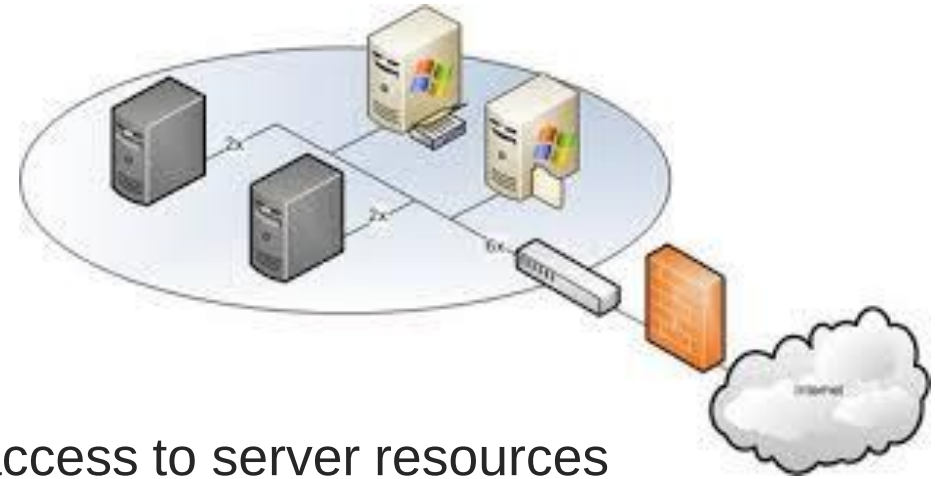
System Administrator



Windows Server Editions

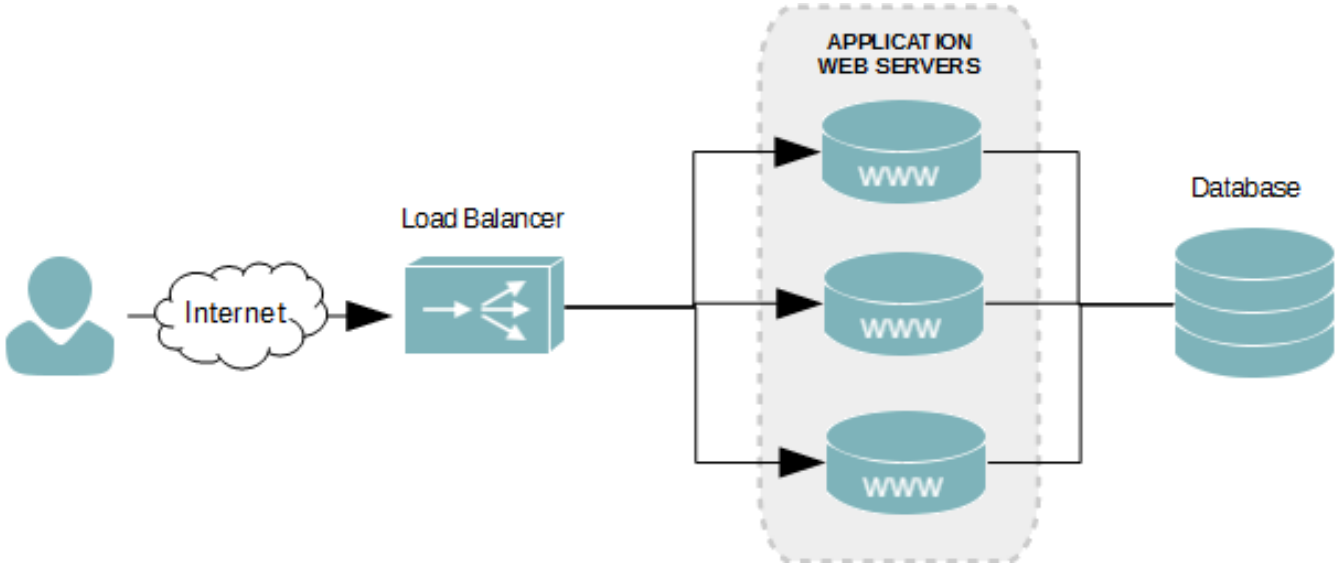
Edition	Ideal for...	Visualization rights	Licensing model	Client Access Licenses	RAM Limit
Essentials	Small businesses with basic IT requirements; very small or no IT department	no, one physical **or** one virtual installation	CPU-based	CALs not required * (limited to 25 users / 50 devices)	64 GB RAM
Standard	For all companies that require advanced features and virtualize to a lesser extent	2 virtual machines ** **or** 2 Hyper-V Container	Core-based	CALs required ***	24 TB RAM
Datacenter	For all companies with high requirements on IT workloads with large number of virtual systems	unlimited virtual machines and Hyper-V Container			

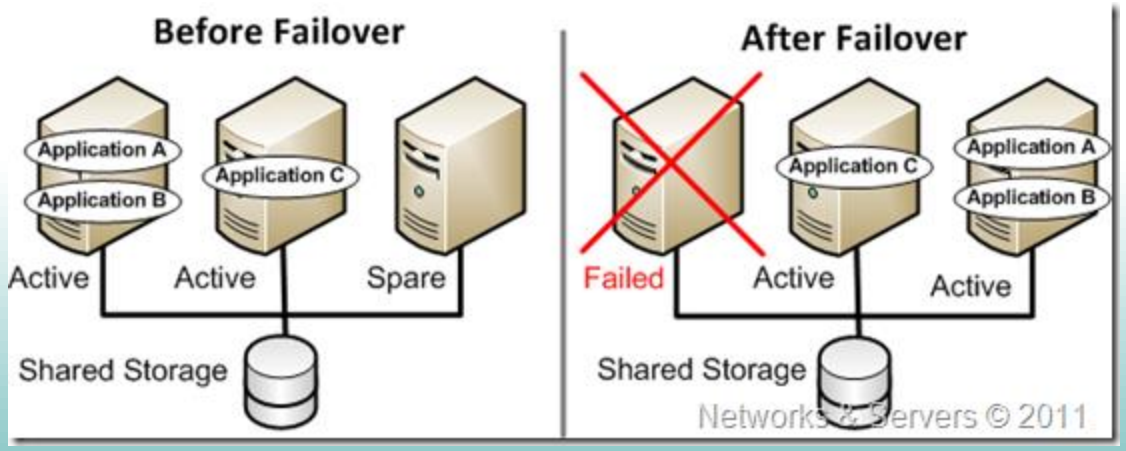
Windows Server Clustering



- **Failover Clustering**
  - The ability to increase the access to server resources and provide fail-safe services
  - By linking two or more discrete computer systems so they appear to function as though they are one
  - Advantages:
    - High availability
    - Increases computer speed to complete server tasks faster
    - Provides more computing power for handling resource-hungry applications

Windows Server Clustering



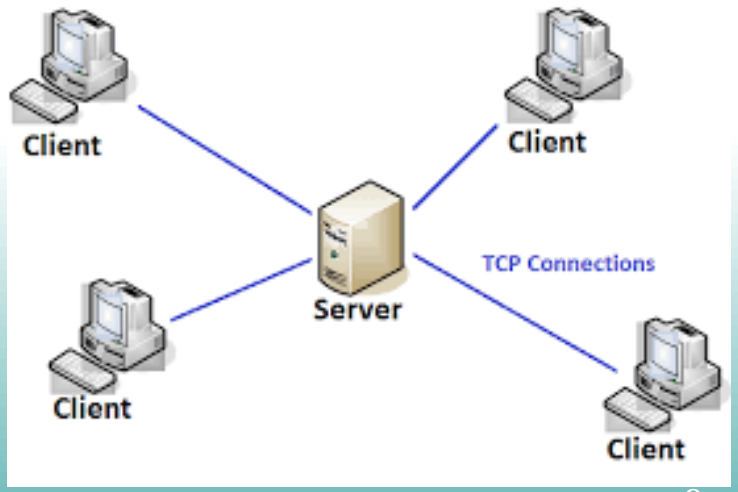


SERVER ROLES

1. Active Directory Certificate Services
2. Active Directory Domain Services
3. Active Directory Federation Services
4. Active Directory Lightweight Directory Services
5. Active Directory Rights Management Services
6. Application Server
7. DHCP Server
8. DNS Server
9. Fax Server
10. File and Storage Services
11. File and iSCSI Services
12. File Server
13. BranchCache for Network Files
14. Data Deduplication
15. DFS Namespaces
16. DFS Replication
17. File Server Resource Manager
18. File Server VSS Agent Services
19. iSCSI Target Server
20. iSCSI Target Storage Provider
21. Server for NFS
22. Storage Services
23. Hyper-V
24. Network Policy and Access Services
25. Print and Document Services
26. Remote Access
27. Remote Desktop Services
28. Volume Activation Services
29. Web Server (IIS)

Using Windows Server with Client Systems

- **Client**
  - A computer that accesses resources on another computer via a network
- **Workstation**
  - A computer that has its own central processing unit (CPU) and can be used as a stand-alone or network computer
- **Thin and Fat Clients**



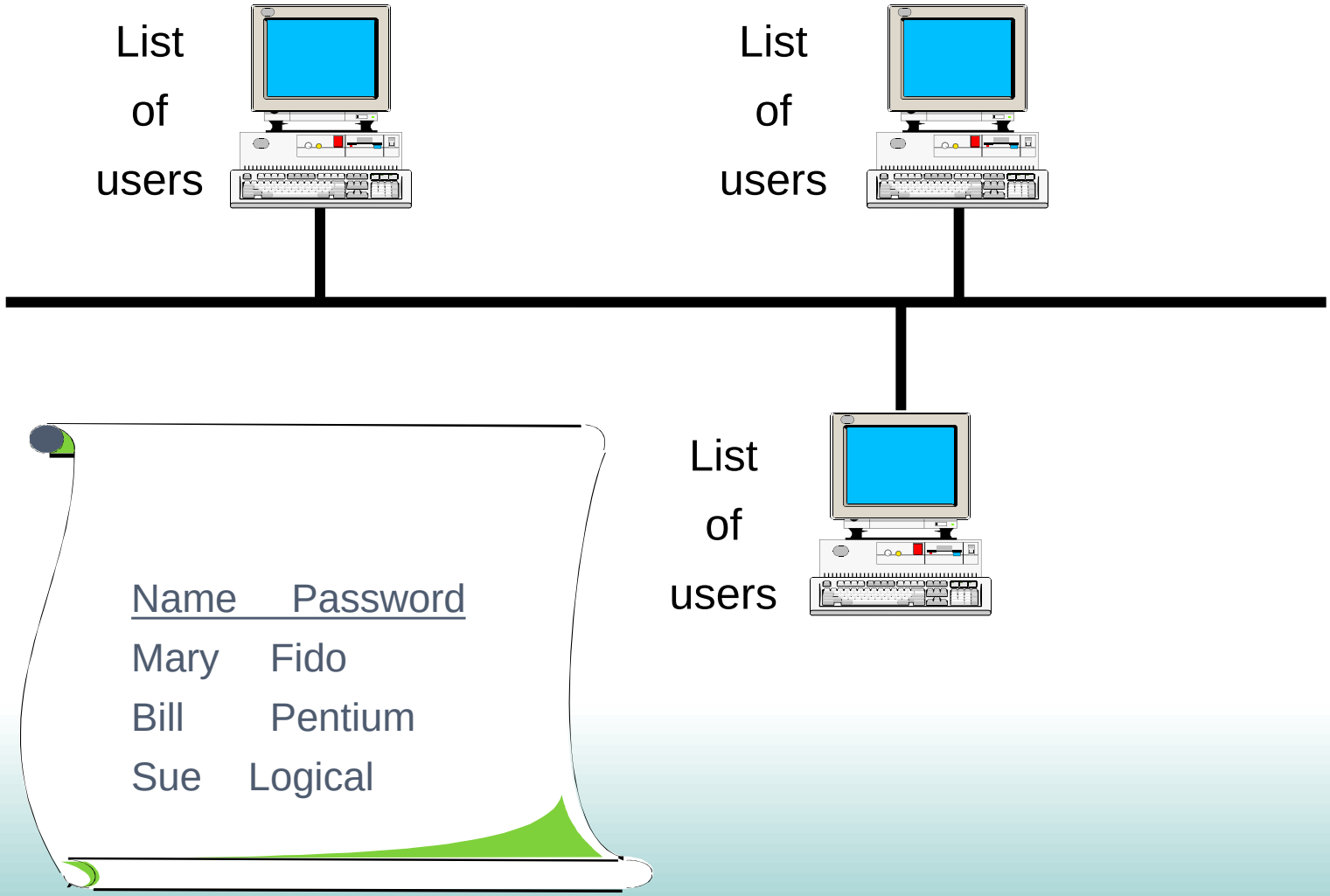
Windows Networking Concepts Overview

- Two different security models used in Windows environments
  1. Workgroup
  2. Domain
- Three roles for a Windows Server in a network:
  1. Standalone server
  2. Member server
  3. Domain controller

Workgroup

- A workgroup is a logical group of computers
  - Characterized by a decentralized security and administration model
  - Authentication provided by a local account database – Security Accounts Manager (SAM)
- Limitations
  - Users need unique accounts on each workstation
  - Users manage their own accounts (security issues)
  - Not very scalable

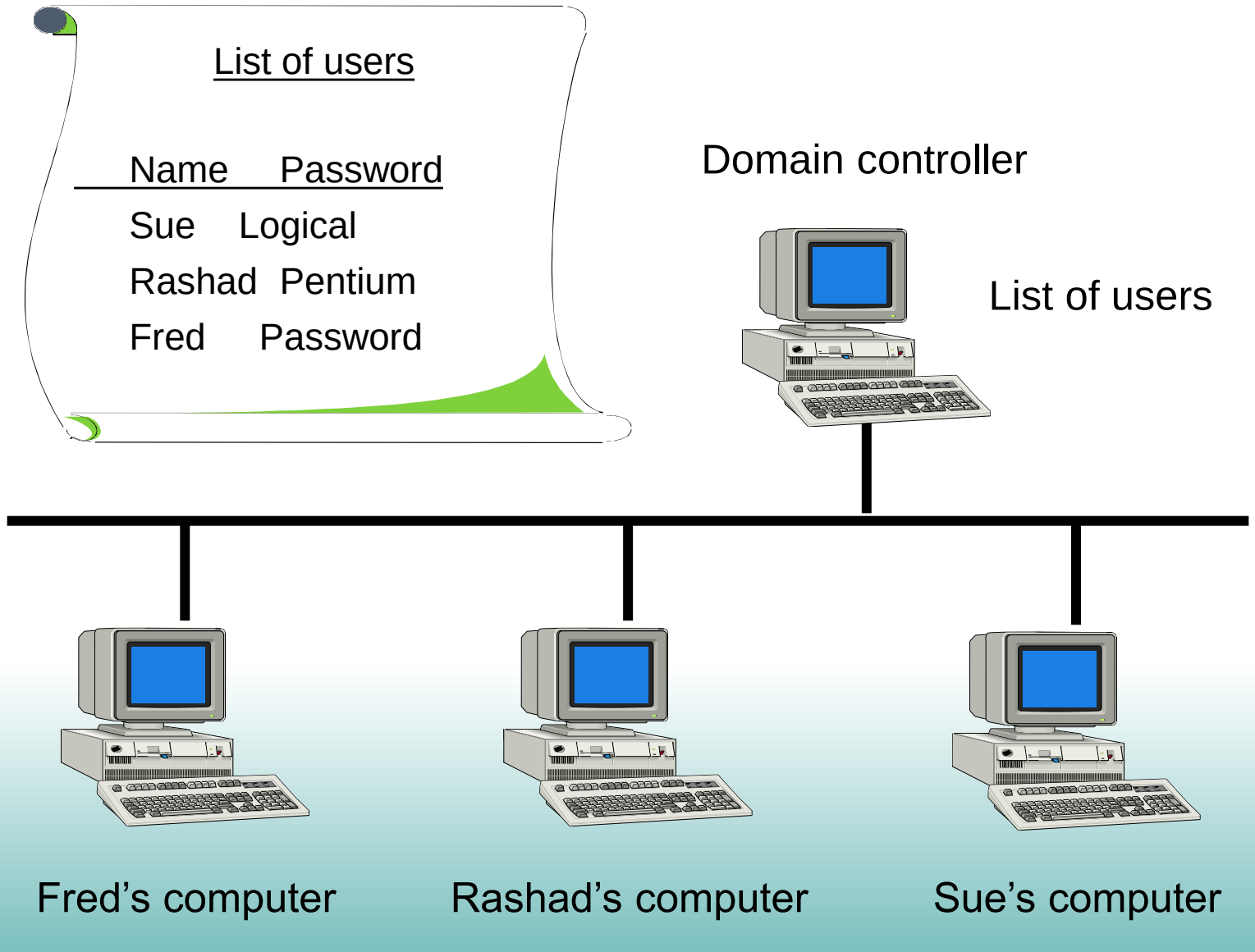
A Workgroup



Domain

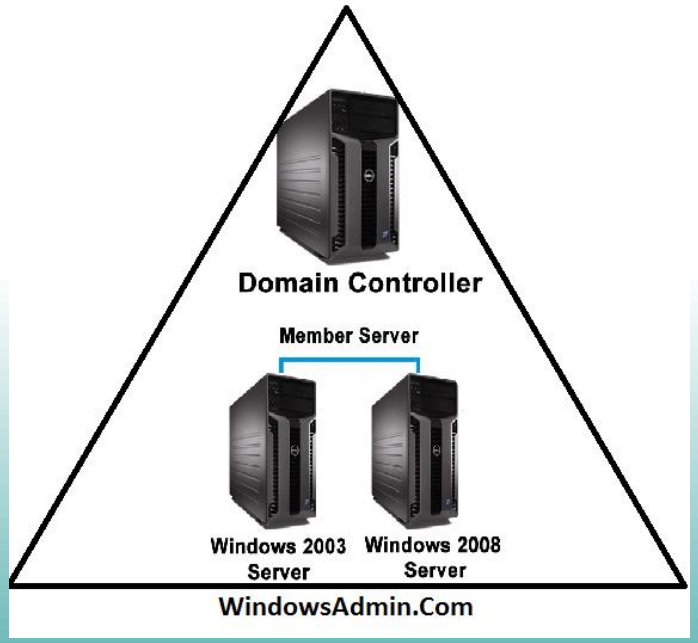
- A domain is a logical group of objects such as computers and user accounts
  - Characterized by centralized authentication and administration
  - Authentication provided through centralized Active Directory
  - Active Directory database can be physically distributed across domain controllers
  - Requires at least one system configured as a domain controller

A domain has a centralized directory database



Member Servers

- A member server
  - Has an account in a domain
  - Is not configured as a domain controller
  - Typically used as a file server, print server, application server, database server, web server and others.



Domain Controllers

- Explicitly configured to store a copy of Active Directory
- Service user authentication requests
- Service queries about domain objects
- May be a dedicated server but is not required to be

Computer Accounts

- Assigned in Windows NT, 2000, XP, Vista, 7, 8, 2003, 2008, 2012, 2016
- Assigned when joining a domain
- Method for authentication and access auditing
- Accounts are represented as computer objects
- Accounts can be viewed using administrative tools
- *Computers running Windows 95 and Windows 98 do not have advanced security features. Therefore, they are not assigned computer accounts.*

Using Active Directory Users and Computers to View a Computer Object

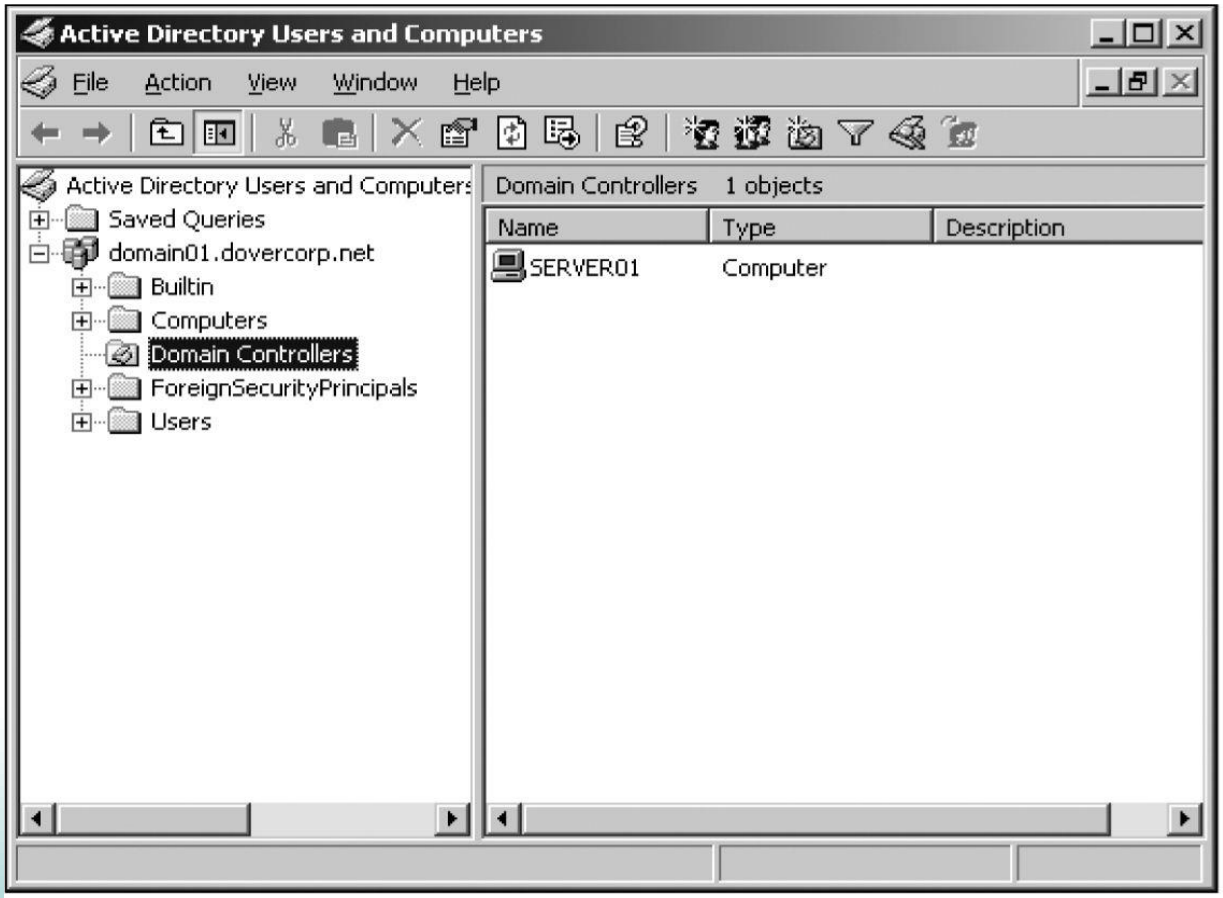


Figure 1-5 Using Active Directory Users and Computers to view a computer object

Diploma in Infocomm & Security

INTRODUCTION TO WINDOWS SERVER ACTIVE DIRECTORY

AD DS (Active Directory Domain Services)

- Provides the following services
  - Central point for storing and managing network objects
    - User accounts, groups, workstations, servers, Group Policies, contacts, printers, shared folders
  - Central point for administration of objects and resources
  - Logon and authentication services
    - Users must authenticate to the domain in which their user account resides before they can access resources, such as shared folders
  - Delegation of administration
- Stored on **Domain Controllers** in the network
- Changes made to any Active Directory will be replicated across all domain controllers
  - Multi master replication
  - Fault tolerance for domain controller failure

Active Directory Objects

- An **object** represents a network resource such as a user, group, computer, or printer
- Objects have attributes depending on object type
- Objects are searchable by attributes

  - Objects
    - Users, groups, printers, computers
  - Attributes
    - Names, phone numbers, locations

- **Schema** – set of rules or blueprint that defines the classes of objects and attributes
- Active Directory is a **DATABASE**.

Active Directory Objects

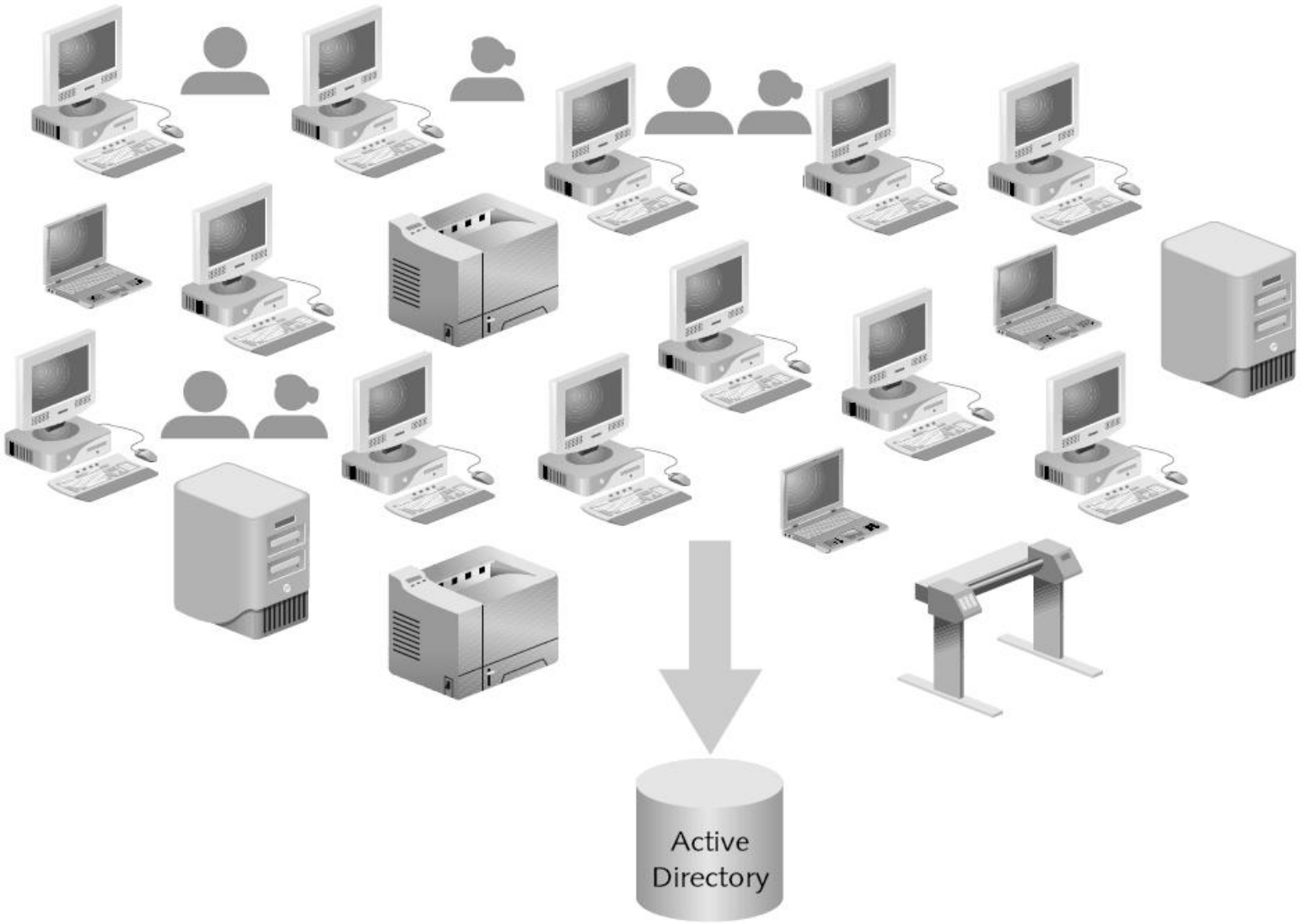


Figure 4-1 Active Directory domain objects include servers, workstations, printers, users, user groups, and other resources.

Active Directory and Domain Controller

- A server with **Active Directory** installed
- Used to administer domain objects, such as user accounts and groups

- All domain controllers are **peers**, and so
  - Any domain controller can be used to administer objects in Active Directory

Domain Functional Levels

- Functional levels determine available AD DS domain or forest **capabilities**.
- Determine which Windows Server **OS** can be run on Domain Controllers in domain or forest.
- DFL (Domain Functional Level) should be same or higher level than FFL (Forest Functional Level)
- Only affects DCs (Domain Controllers)

Domain Functional Level

Domain Functional Level	Supported Domain Controller OS
Windows Server 2008	Windows Server 2008, 2008 R2 Windows Server 2012, 2012 R2, 2016
Windows Server 2008 R2	Windows Server 2008 R2 Windows Server 2012, 2012 R2, 2016
Windows Server 2012	Windows Server 2012, 2012 R2, 2016
Windows Server 2012 R2	Windows Server 2012, 2012 R2, 2016
Windows Server 2016	Windows Server 2016

Domains and Organizational Units

- **Domain**
  - Has a unique name
  - Is organized in hierarchical levels
  - Has an Active Directory replicated across its domain controllers
- **Organizational unit (OU)**
  - A logical container used to organize domain objects
  - Makes it easy to locate and manage objects
  - Allows you to apply **Group Policy** settings
  - Allows delegation of administrative control
    - A user can be assigned the task of resetting passwords for the accounts without having to grant that user administrative rights in the domain
  - By default, there is only one OU created in AD, the Domain Controller OU

Organizational Unit

- When you plan to create OUs, keep three concerns in mind:
  1. Microsoft recommends that you limit OUs to 10 levels or fewer
  2. Active Directory works more efficiently when OUs are set up horizontally instead of vertically
  3. The creation of OUs involves more processing resources because each request through an OU requires CPU time

An Active Directory Domain and OU Structure

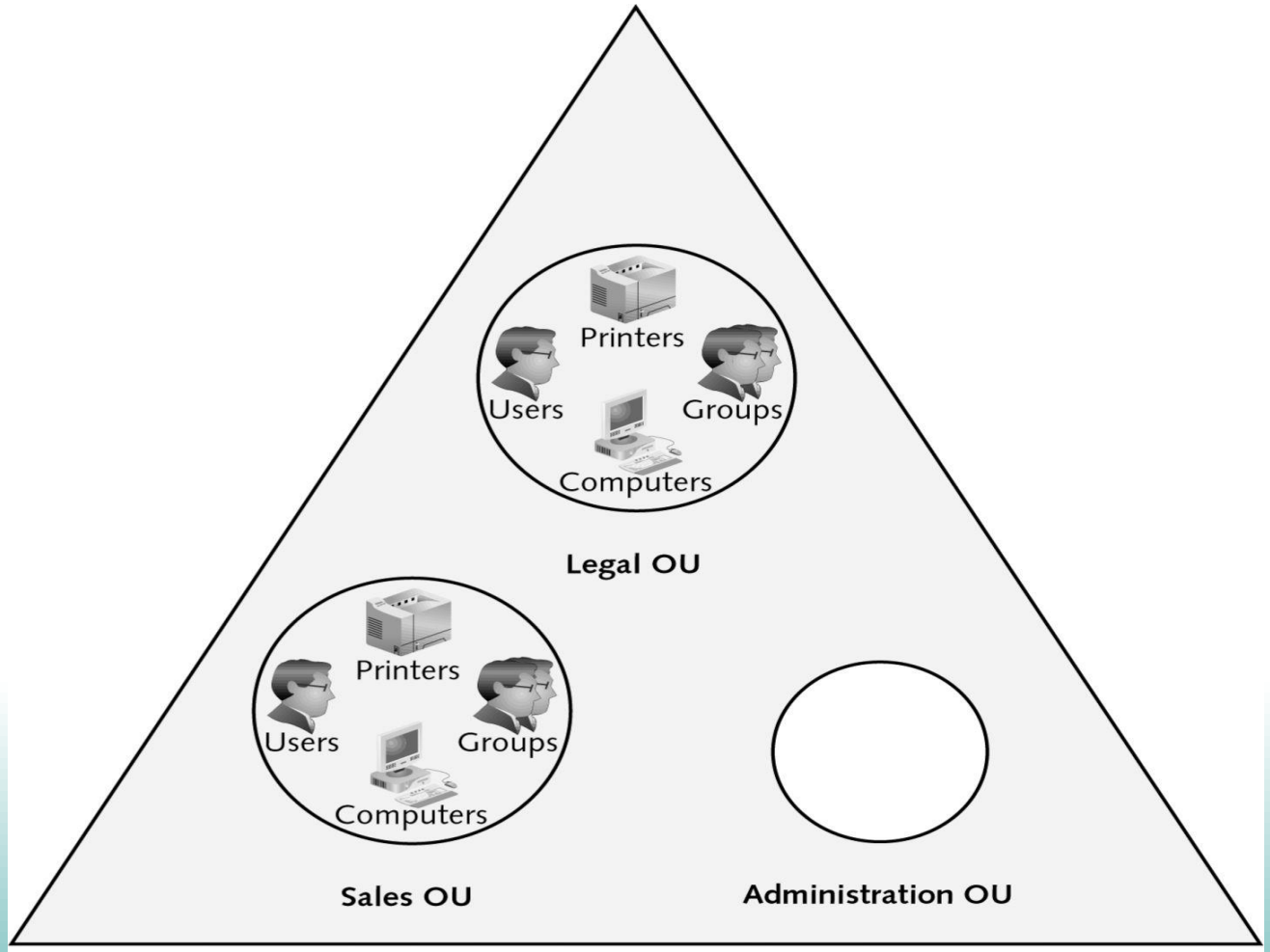


Figure 1-14 An Active Directory domain and OU structure

Trees and Forests

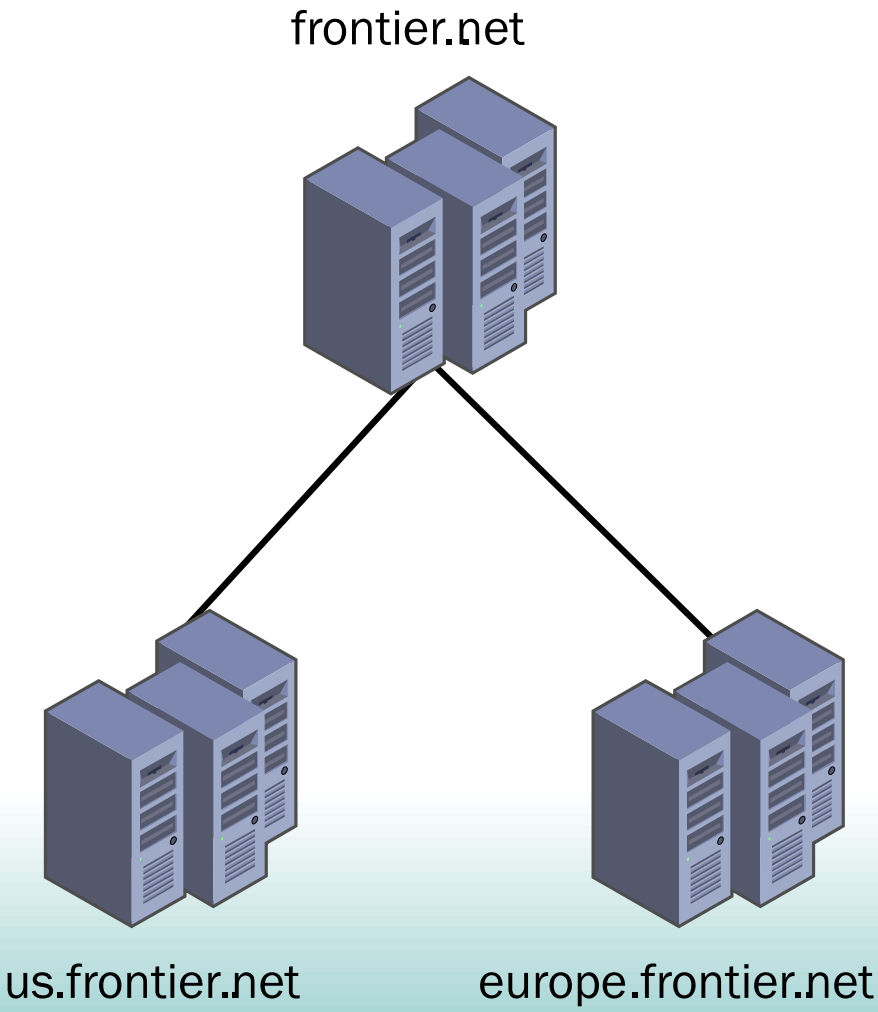
- Sometimes necessary to create multiple domains within an organization
- First Active Directory domain is the **forest root domain**
- A **tree** is a hierarchical collection of domains that share a contiguous DNS naming structure
- A **forest** is a collection of trees that do not share a contiguous DNS naming structure
  - All domains in the forest share a common schema
- **Transitive trust** relationships exist among domains in trees and, optionally, in and across forests

Tree

- Contains one or more domains that are in a common relationship

- Tree has the following characteristics:
  - Domains are represented in a contiguous namespace and can be in a hierarchy
  - Two-way trust relationships exist between parent domains and child domains
  - All domains in a single tree use the same schema for all types of common objects
  - All domains use the same global catalog

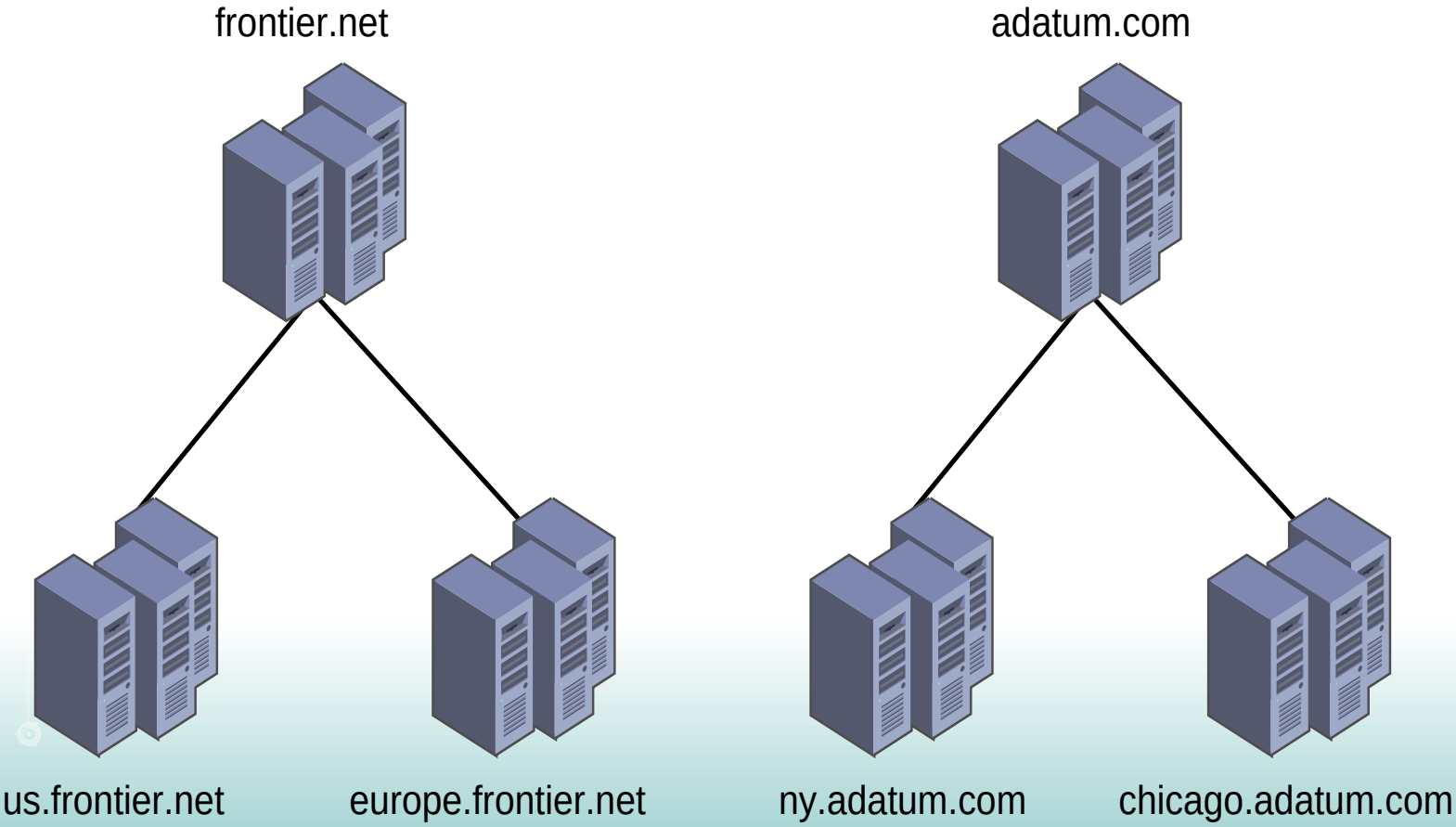
Active Directory Tree



Forest

- **Forest**
  - Consists of one or more Active Directory trees that are in a common relationship
- Forests have the following characteristics:
  - The trees can use a disjointed namespace
  - All trees use the same schema
  - All trees use the same global catalog
  - Domains enable administration of commonly associated objects, such as accounts and other resources, within a forest
  - Two-way transitive trusts are automatically configured between domains within a single forest

Active Directory Forest



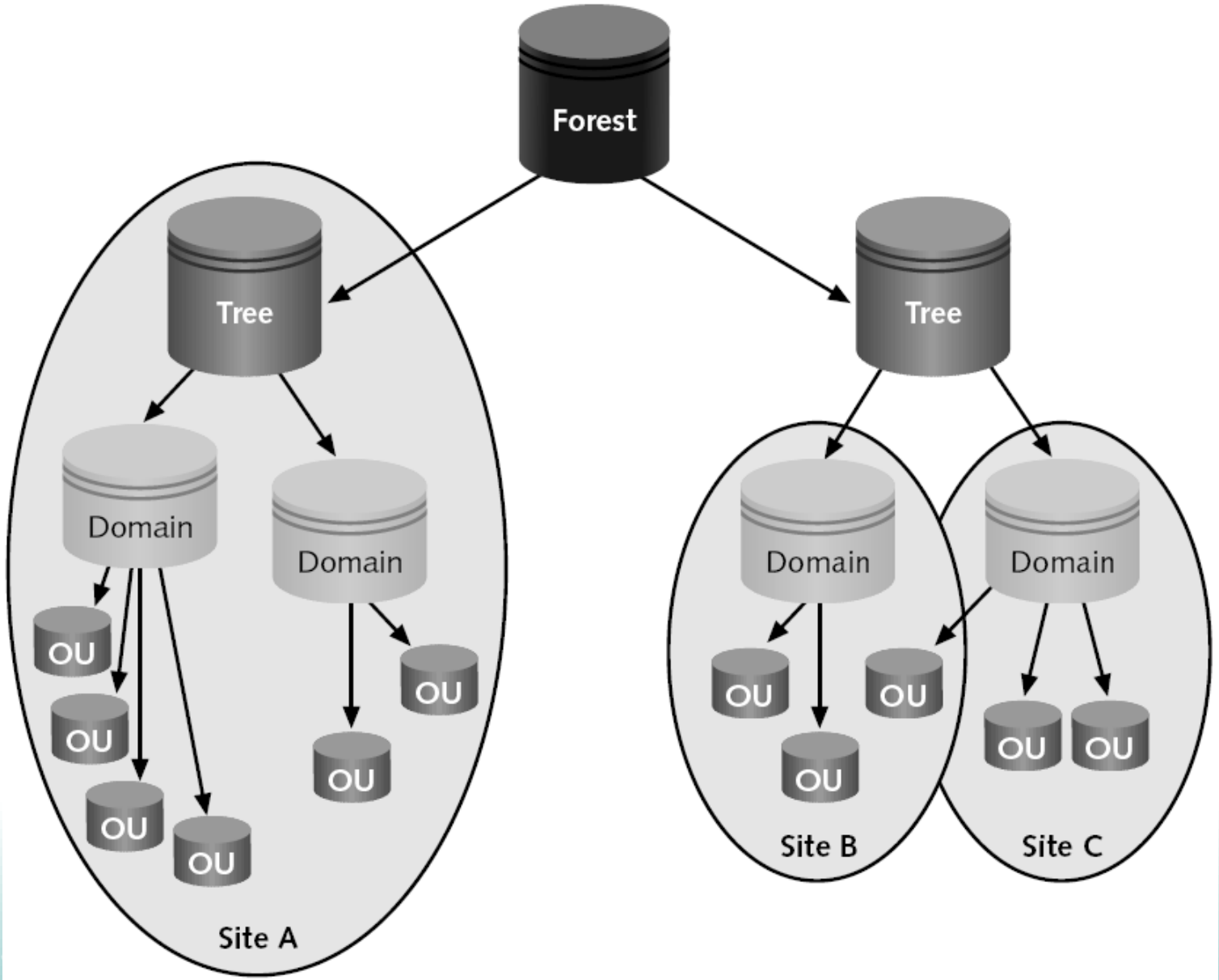


Figure 4-5 Active Directory hierarchical containers

Global Catalog

- **Global catalog**
  - Stores information about every object within a forest
  - Store a full replica of every object within its own domain and a partial replica of each object within every domain in the forest
- The first DC configured in a forest becomes the global catalog server
- The global catalog server enables forest-wide searches of data

Active Directory Communications Standards

- The **Lightweight Directory Access Protocol** (LDAP) is used to query or update Active Directory database directly
- LDAP follows convention using naming paths with two components
  - Distinguished name: the unique name of an object in Active Directory (CN=Joe,OU=Sales,DC=Frontier,DC=net)
  - Relative distinguished name: the portion of a distinguished name that is unique within the context of its container (OU=Sales)

Summary

- Windows Server network administration goals:
  - Make network resources available to users as permitted
  - Secure the network from unauthorized access
- Several editions of Windows Server with different features and costs
- Two network security models – Workgroup & Domain
- Three possible server roles – Standalone, Member, Domain Controller
- Domain, Organizational Unit (OU)
- Tree, Forest concepts.
- Active Directory