Active Directory

Hussain Ali
hussain@ccse.kfupm.edu.sa
Department of Computer Engineering

KFUPM, Dhahran, Saudi Arabia

Outline

- Introduction to Active Directory
- Logical Structure
  - » Domain, Organizational Units, Trees and Forests, Schema
- Physical Structure
  - » Sites
  - » Domain Controllers
  - » Specific Domain Controller Roles
- Installing Active Directory

Introduction

- Directory ?
  - » A directory is an information source used to store information about interesting objects. Ex: Telephone directory
  - » A directory service differs from a directory in that it is both the directory information source and the services making the information available and usable to the users.

Need for Directory Service

- Why Have a Directory Service?
  - » Enforce security defined by administrators
  - » Distribute a directory across many computers
  - » Replicate a directory to make it available to more users and resistant to failure
  - » Partition a directory into multiple stores to allow the storage of a very large number of objects

Active Directory Features

- What is the Active Directory?
  - » Directory Service included with Windows 2000
  - » It is secure, distributed, partitioned
  - » It uses multi-master replication
  - » Scalable: No restriction on size of objects
  - » It replaces the SAM database of Windows NT
  - » It can go upto million of objects. NT supports 25,000 users (40MB SAM size).
  - » Organizes information hierarchically to ease network use and management.

Active Directory Features

- Features
  - » DNS Integration
  - » Dynamic DNS
  - » Access to the Active Directory (LDAP, X.500, MAPI-RPC)
  - » Application Programming Interface
  - » Directory Service Functionality
    - ï AD provides central organization, management and control of access to network resources.
  - » Centralized Management
    - ï Single point administration
    - ï Single sign on I.e. users log on once for full access to resources throughout directory

Supported Technologies

- TCP/IP: Network transport
- DHCP: Dynamic Host Control Protocol
- DNS: Domain Name System
- SNTP: Simple Network Time Protocol
- LDAP: Lightweight Director Access Protocol v3
- LDIF: LDAP data interchange format
- Kerberos v5 for authentication
- X.509 certificates for authentication

Naming Convention

- Distinguished Name (DN)
  - » **CN**=Kareem, **CN**=Users,**DC**=ccse,**DC**=kfupm,**DC**=edu, **DC**=sa

  Where CN=common name

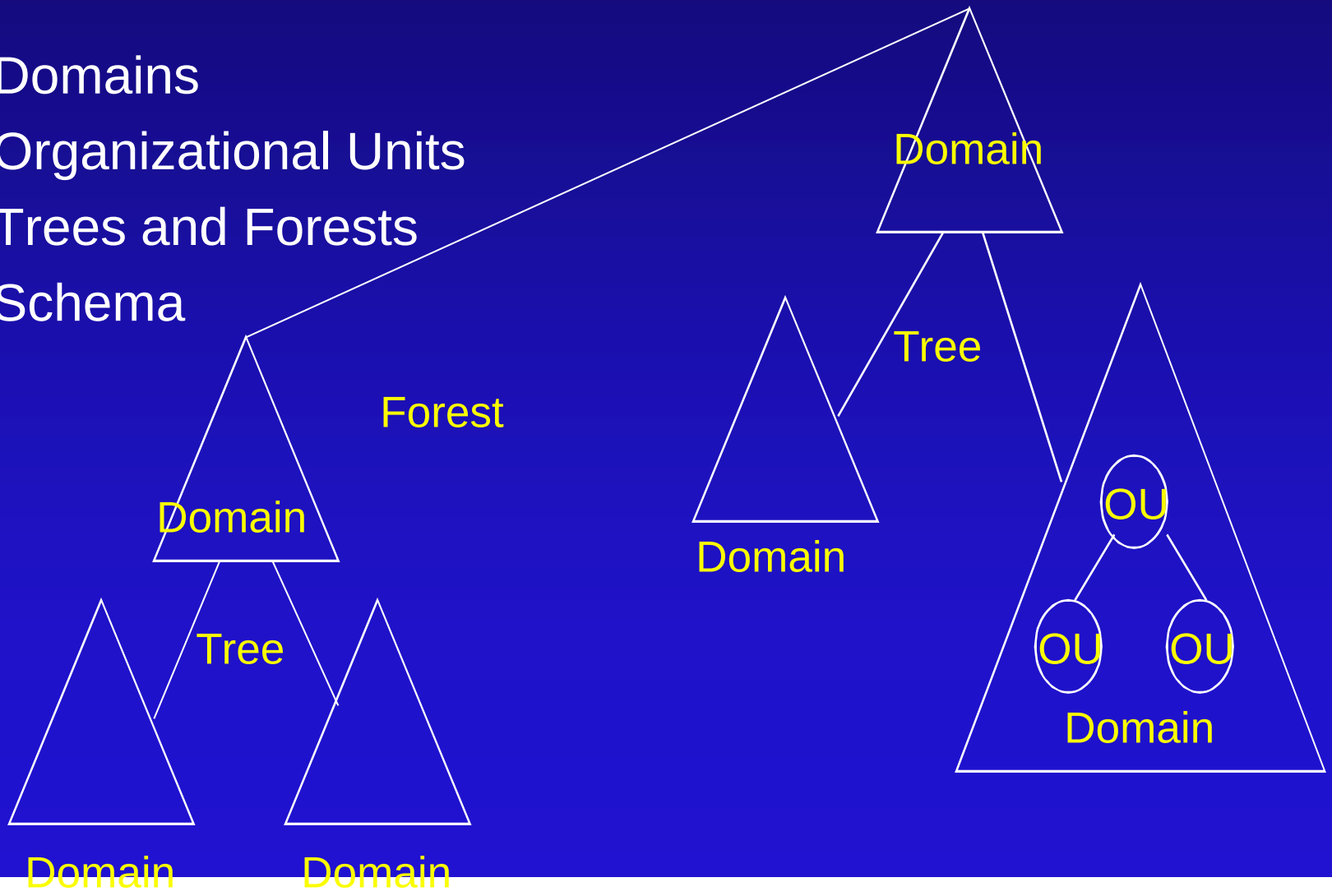
  DC=domain component
- Relative DN
  - » Attribute of the object
  - » Ex: RDN of the Kareem user object is Kareem and RDN for parent object is Users.

Naming Convention

- User Principal Name
  - » UPN of a user object is composed of the user's logon name and DNS name of the domain.
  - » Ex: kareem@ccse.kfupm.edu.sa
- Globally Unique Identifier (GUIDs)
  - » GUID is a 128-bit hexadecimal representation to objects
- Uniqueness of Names
  - » DN are guaranteed to be unique in the forest

Logical Structure

- Domains
- Organizational Units
- Trees and Forests
- Schema



Logical Structure

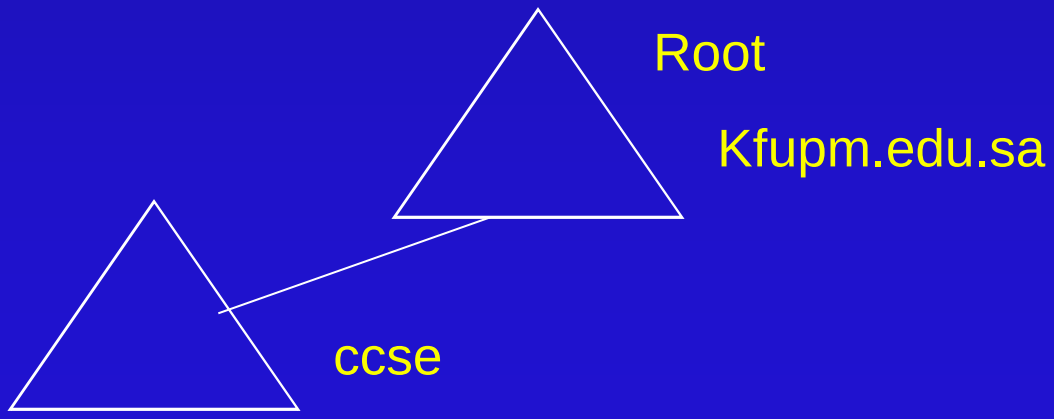
- Domains
  - Security Boundary
  - Unit of Replication
  - Multi-Master replication model
  - Domain Modes
    - Mixed mode (Windows 2000 & NT controllers)
    - Native mode (Windows 2000 controllers only)

Logical Structure

- Organization Units
  - » Organization Unit (OU) is a container object that is used to organize objects within a domain. It contains user accounts, groups, computers, printers and other OUs.
- OU Hierarchy
  - » Organization structure based on department or geographical boundaries
  - » Organization structure based on administrative responsibilities like users, computers etc.
- Administrative Control
  - » OU administrative control can be delegated over the objects within the OU.

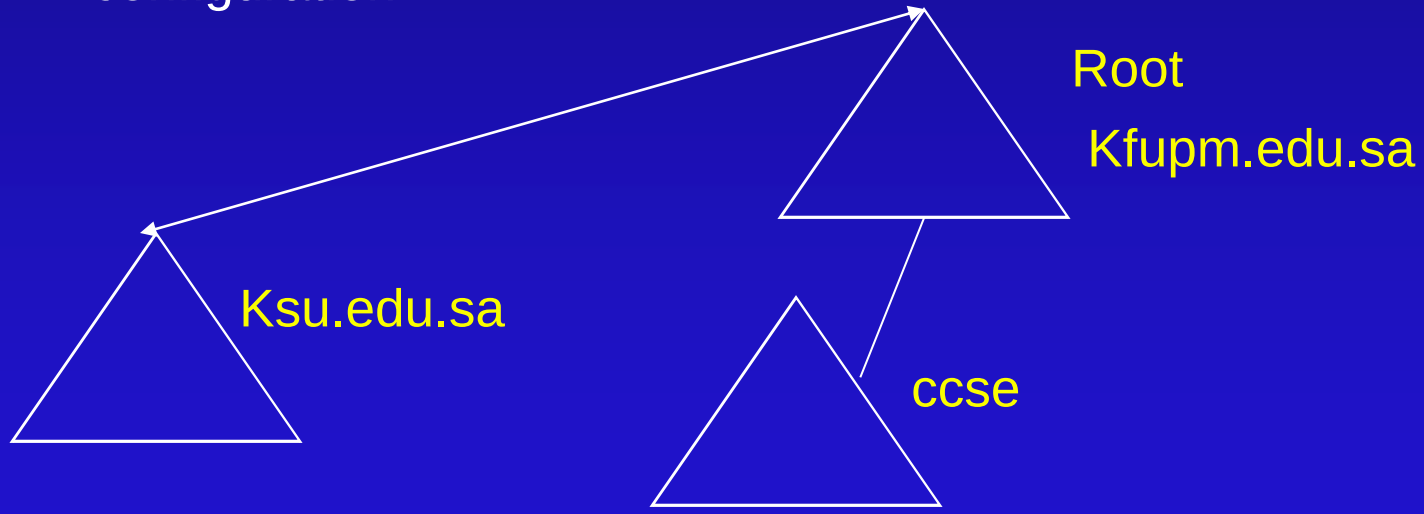
Logical Structure

- Trees
  - A tree is a hierarchical arrangement of Windows 2000 domains that share a contiguous namespace.
  - While adding a domain to an existing tree, the new domain is a child domain of an existing parent domain.



Logical Structure

- Forests
  - » A forest is a group of trees that do not share a contiquous namespace. The trees in a forest share a common configuration.

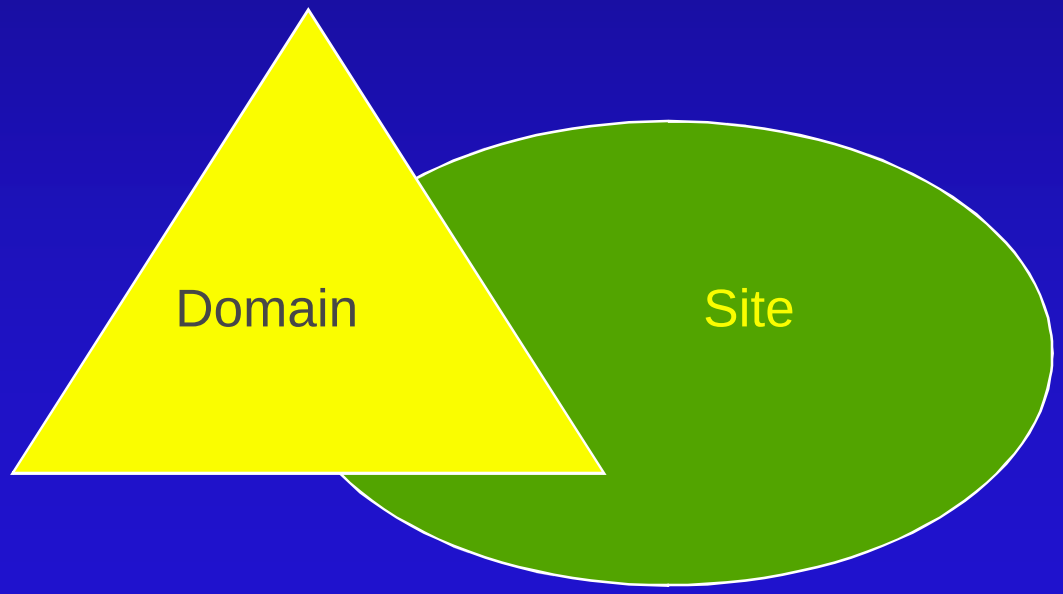


Logical Structure

- Schema
  - » It contains the definitions of all objects such as users, computers and printers.
  - » Two types of definitions: Classes and attributes
  - » Examples:
    - ï Classes: Computers, Users and Servers
    - ï Attribute: accountExpires, mail, Name, badPasswordTime etcé .
  - » Only one schema for the entire forest so that all objects created in AD conform to the same rules
  - » Schema is stored in a database.

Physical Structure

- Sites
- Domain Controllers



Domain Controller Roles

- Global Catalog Server (GCS)
  - » Global Catalog is Repository of information that contains a subset of attributes for all objects in Active Directory.
  - » Most frequent used attributes are stored in GC.
  - » GCS is a domain controller that stores a copy of an processes queries to the global catalog.
  - » It enables a user to find directory information in the entire forest, regardless of the location of the data.

Domain Controller Roles

- Single Master Operations
  - » Schema Master
  - » Domain Naming Master
  - » RID Master
  - » PDC Emulator
  - » Infrastructure Master