# *Active Directory*

By: Kishor Datar

10/25/2007

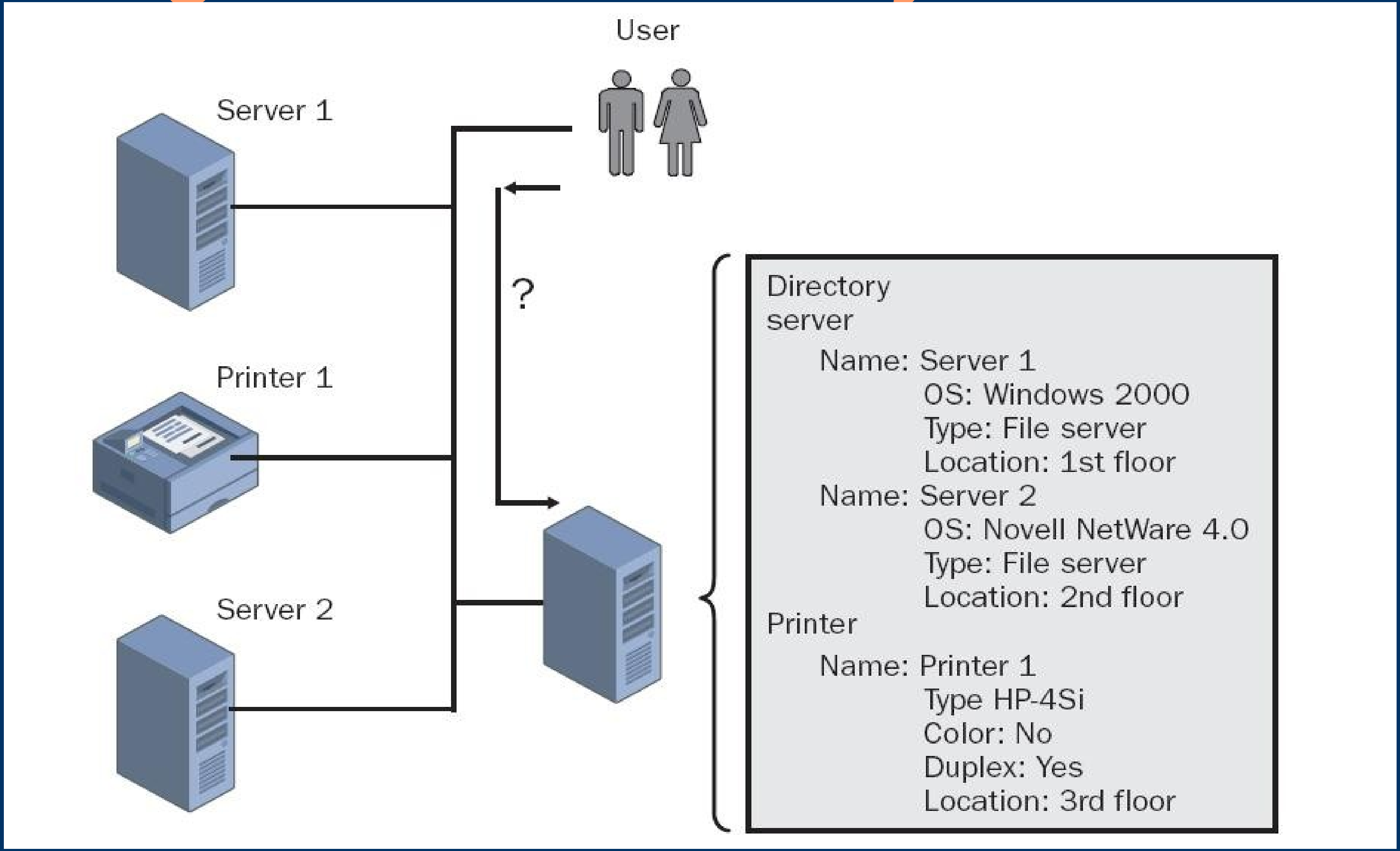
# What is a directory service?

- Directory
  - Collection of related objects
  - Files, Printers, Fax servers etc.
- Directory Service
  - Information needed to use and manage the objects.
  - Source and Mechanism
  - Active Directory is a directory service in Windows 2003 Server

# *Need for a directory service*

- Organize
- Simplify access
- Find objects based on characteristics
- Simple administration
  - Patches
  - Security policies
  - Installation

# Using Active Directory



Directory server
  Name: Server 1
    OS: Windows 2000
    Type: File server
    Location: 1st floor
  Name: Server 2
    OS: Novell NetWare 4.0
    Type: File server
    Location: 2nd floor
Printer
  Name: Printer 1
    Type HP-4Si
    Color: No
    Duplex: Yes
    Location: 3rd floor

Image courtesy of Windows 2003 active directory infrastructure, Spealman et al

# *Features*

- Centralized data store
- Scalability
- Extensibility
- Manageability
- Integration with DNS
- Client configuration management
- Policy based administration
- Replication of information
- Secure authentication and authorization

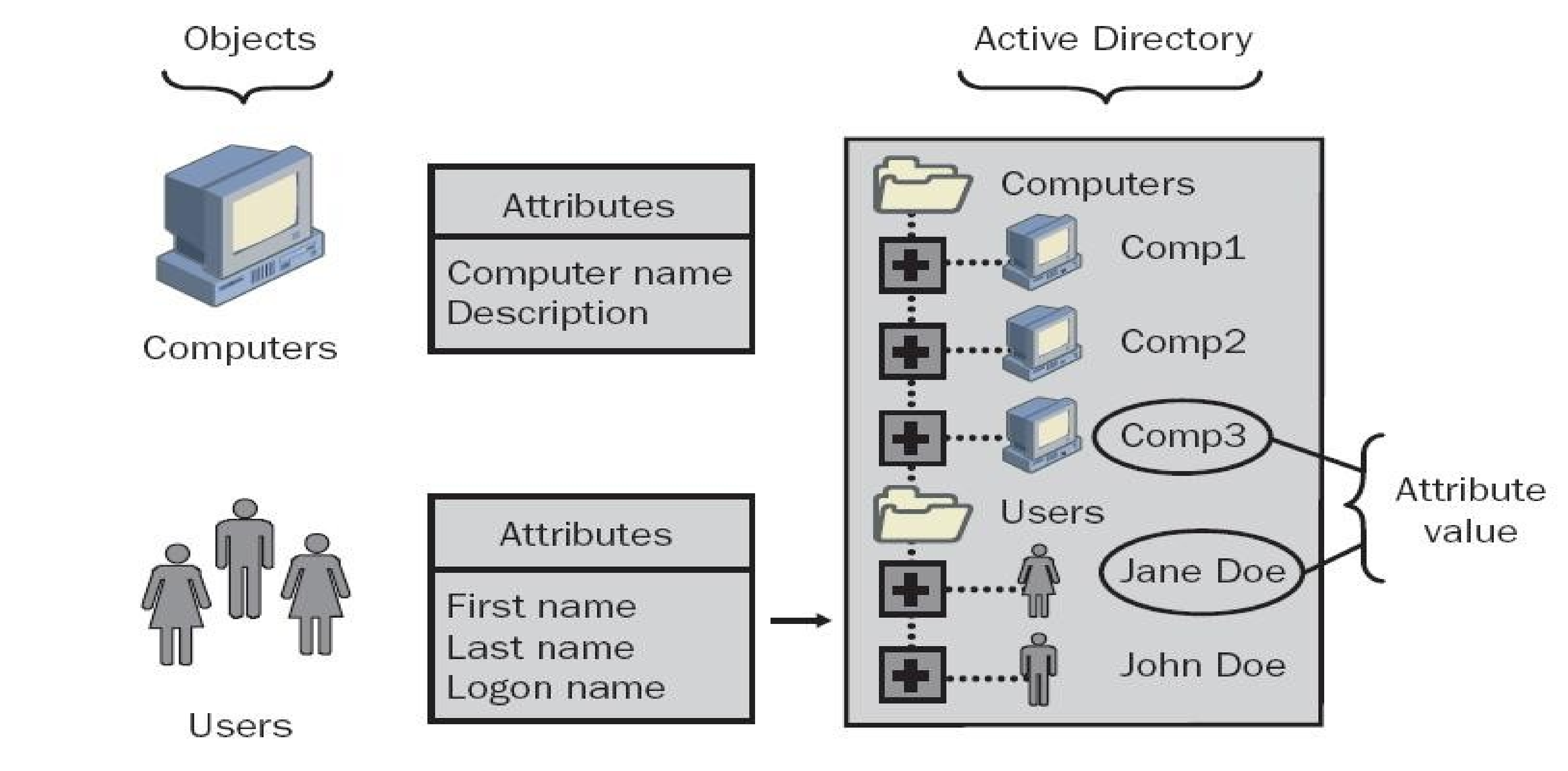
# *Features.. continued..*

- Secure integration
- Interoperability with other directory services
- Signed and encrypted LDAP traffic

# *Active Directory Objects*

- Data stored is organized into objects
- Named set of attributes
- Represent resource
- Container objects .. Figure 2
- Schema
  - Define Objects, are objects themselves
  - Schema Objects = Class Objects + Attribute Objects
  - Extending schema, caution, test forest

# Objects and attributes



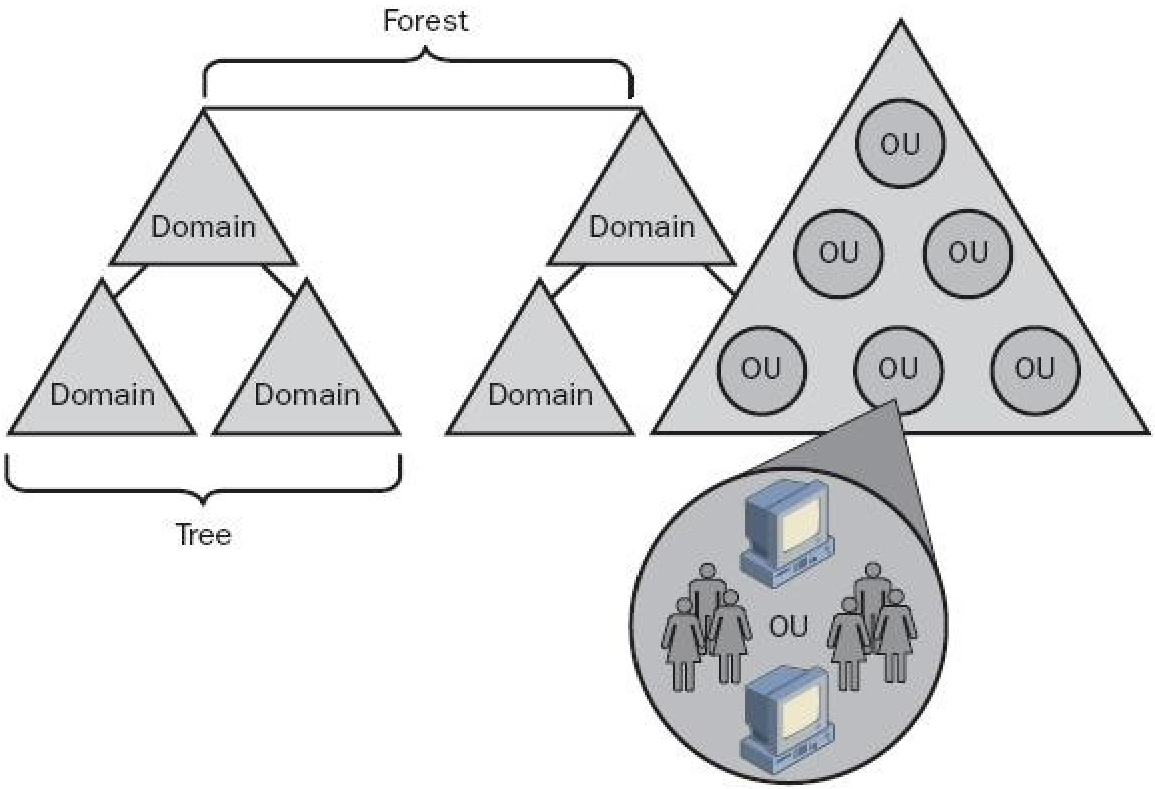
Active Directory objects and attributes

Image courtesy of Windows 2003 active directory infrastructure, Spealman et al

# *Components*

- Logical structure
  - Domains
  - Organizational units
  - Trees
  - Forests
- Physical structure
  - Sites
  - Domain Controller

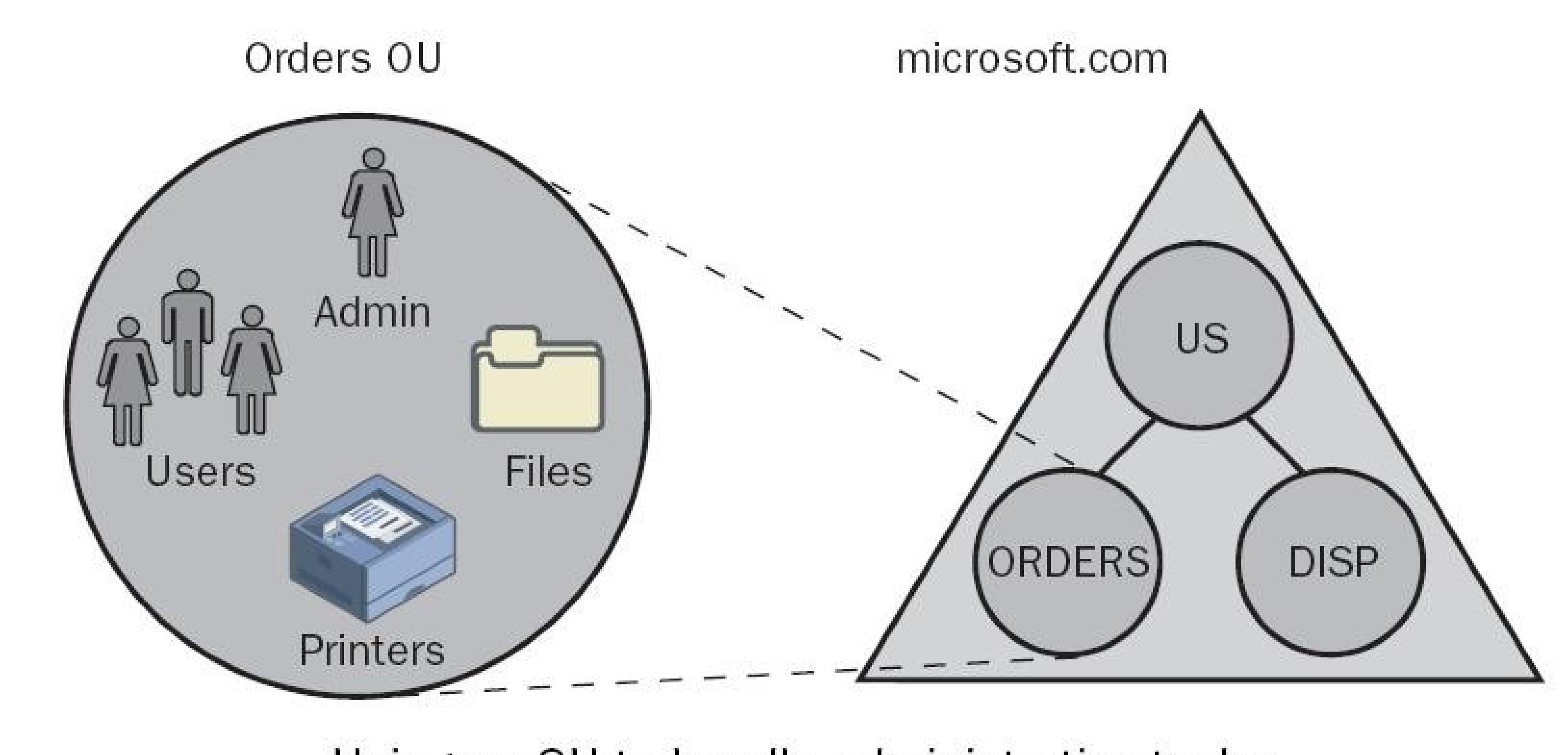
# Logical Structures



The relationship of Active Directory domains, OUs, trees, and forests

Image courtesy of Windows 2003 active directory infrastructure, Spealman et al

# OUs



Using an OU to handle administrative tasks

Image courtesy of Windows 2003 active directory infrastructure, Spealman et al

# Domain Trees

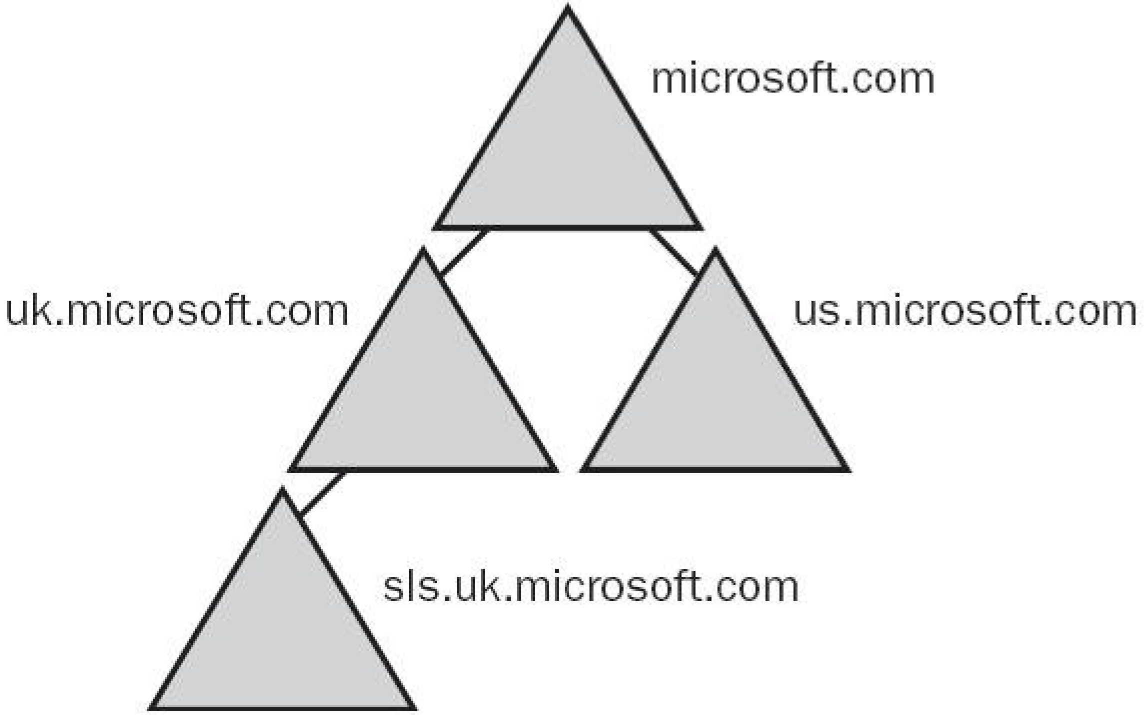


**Figure 1-6** A domain tree

Image courtesy of Windows 2003 active directory infrastructure, Spealman et al

# *Physical Structure*

- Sites

- Domain Controller

# *Sites*

- Combination of one or more IP subnets connected by a “Fast Link”
- Typically has same boundaries as LANs
- Are not part of the namespace
- Computer Objects and Connection Objects

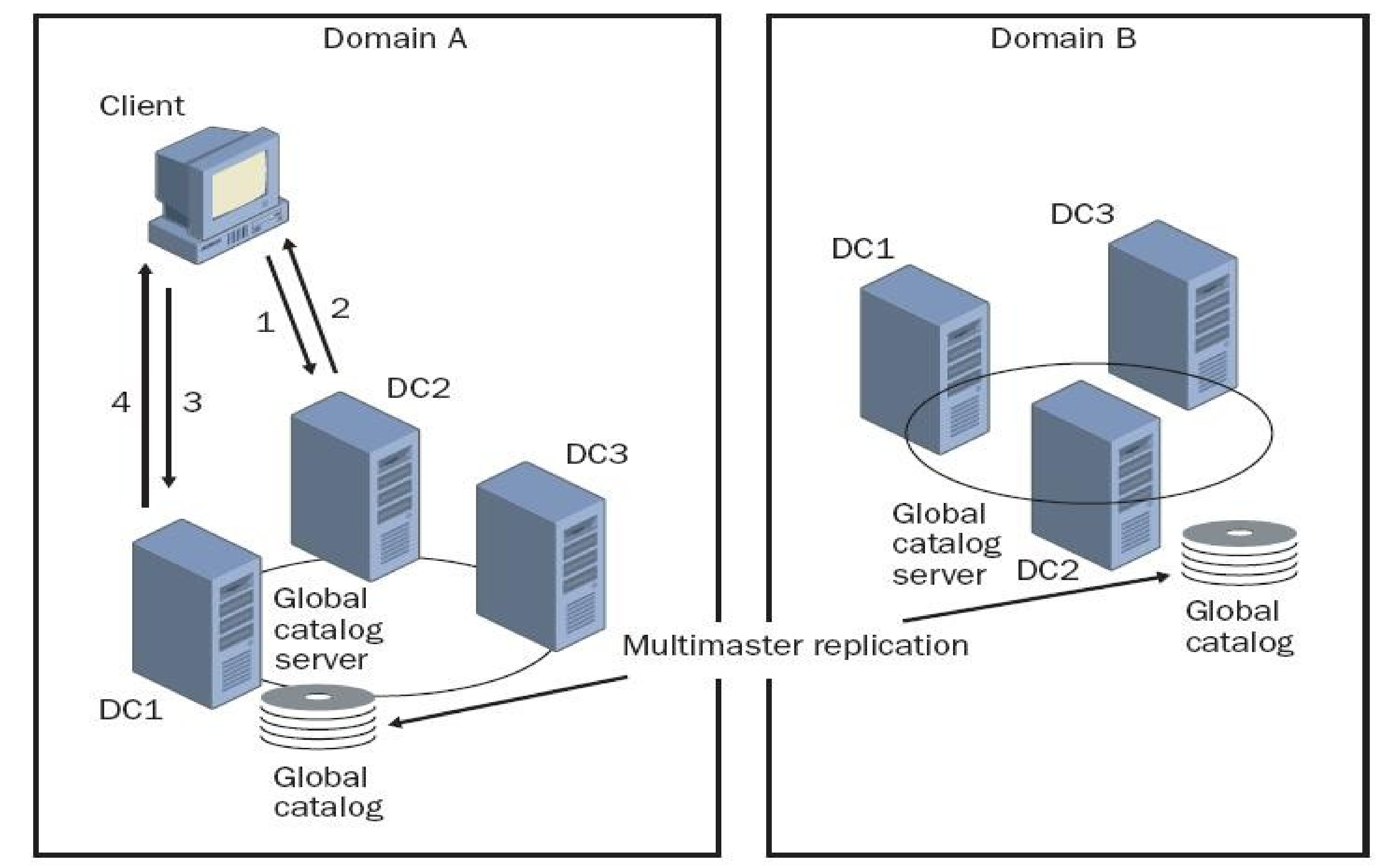
# Domain Controllers

- Windows Server 2003
- Functions
  - Store complete copy of information, manages changes and replication
  - Multi-master replication: All DCs are peers
  - Practically – operations master is used
  - Detect collision due to modification of attribute, resolved by use of higher property version number
  - Locate objects, validate user logon attempts

# *Catalog services – The global catalog*

- Selected information about every object in all domains in a directory
- Full replica of all object attributes for its host domain, partial replica for every domain
- Functions:
  - Enables users to logon (Universal Group Membership)
  - Finding information
  - Provides Universal Group Membership info to DC

# Query Process



Retrieve, Modify, Delete information

Port 3268 of DC

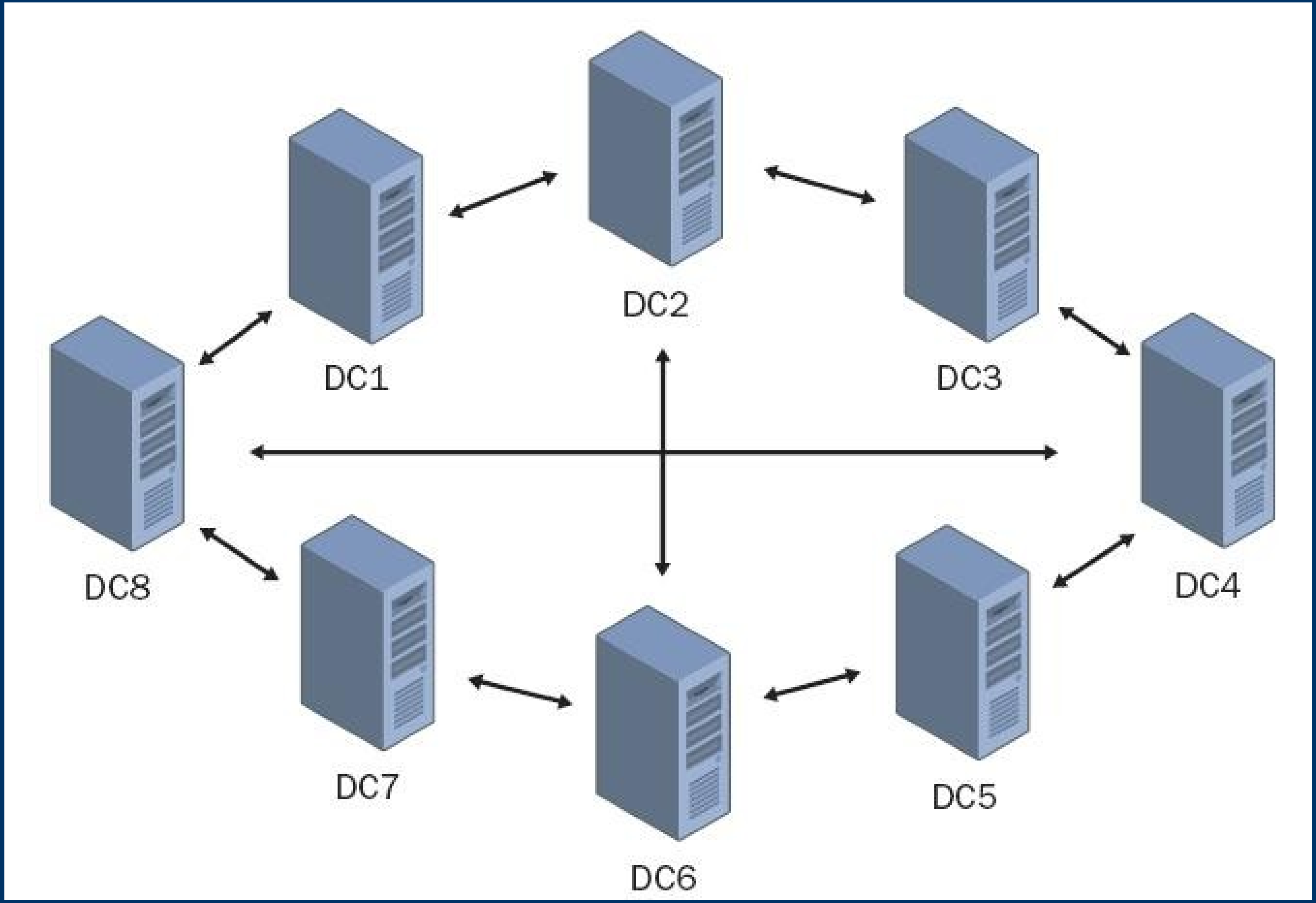
Standard Queries on 389

Image courtesy of Windows 2003 active directory infrastructure, Spealman et al

# What information is replicated

- Schema Partition (DC & GC)
- Configuration Partition (DC & GC)
- Domain Partition (DC)
- Application Directory Partition
- Ntds.dit file

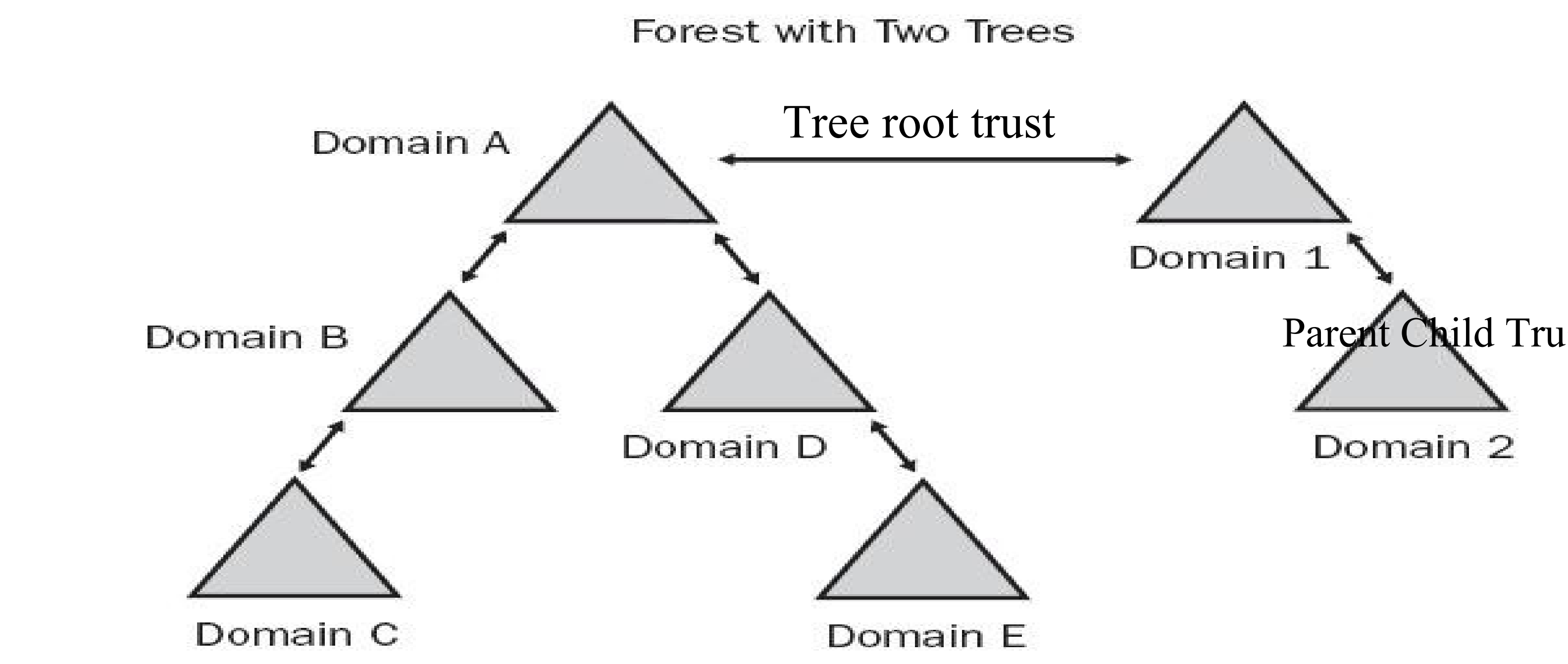
# *Intrasite Replication*



- No more than 3 hops
- 2 Paths
- KCC
- Replication Partners
- Intersite Replication (Site Links)

# *Trust and Trust Relationship*

- Kerberos, NTLM
- Method of Creation, Transitivity, Direction
- Shortcut,External,Forest,Realm Trust



# *Change and Configuration Management and IntelliMirror*

- User Data Management
- S/W installation and maintenance
- User settings management
- Computer settings management
- Remote installation services

# Group Policies

- Group Policies

- GPOs
  - How are the applied
    - Local GPO
    - GPOs linked to site
    - GPOs linked to domains
    - GPOs linked to OUs (Highest level OU first)

# DNS & Object Naming

- User friendly names
- Connect to local servers using same naming convention as Internet
- LDAP
- Distinguished Name (DN) - Unique
  - CN=Deepak, OU=Promotions, OU=Marketing, DC= umbc, DC=edu
- RDN
- GUIDs
- UPN

# *Few Examples,*

- To disable multiple computer accounts,
  - dsmod computer CN=MemberServer1, CN=Computers,DC=Microsoft,DC=Com -disbled yes
- To find all contacts in the current domain whose names start with "te"
  - dsquery contact domainroot -name te*
- To Create an Organizational Unit
  - dsadd ou "ou=guyds, dc=cp, dc=com"

# Review

- Basic Concepts
- Purpose of using AD
- Physical and logical structure
- Group policies
- Trust relationships
- Replication strategies
- Naming
- Examples

# *Questions?*

- ?

- ?

# References

- [1] Book: Microsoft Windows Server 2003 Active Directory infrastructure [Spealman et al]
- [2] http://www.microsoft.com/
- [3] A Guide to Microsoft Active Directory (AD) Design [John Dias]
- [4] http://www.computerperformance.co.uk/