Active Directory

(March 30, 2016)

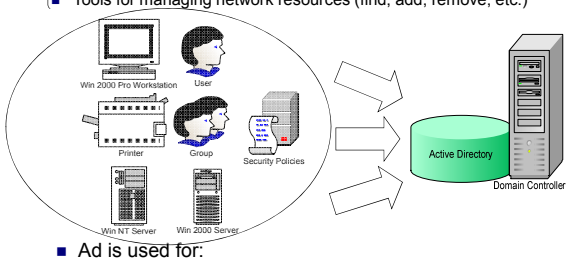
© Abdou Illia, Spring 2016

Learning Objective

- Use Active Directory concepts
  - Namespace
  - DNS
  - Global Catalog
  - Schema
  - Class
  - Tree
  - Forest
  - Organizational Units

Active Directory

AD =
- A Central Database on a Domain Controller for storing network resources and security policies +
- Tools for managing network resources (find, add, remove, etc.)



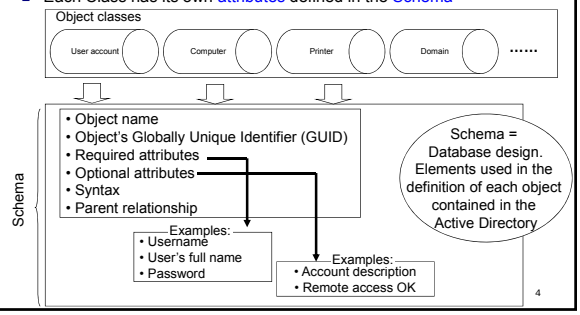
- Ad is used for:
  - Resource lookup (Searching for specific resources)
  - User authentication (login)

Active Directory structure

- Individual resources are called objects
- Objects belong to classes
- Each Class has its own attributes defined in the Schema

Default classes

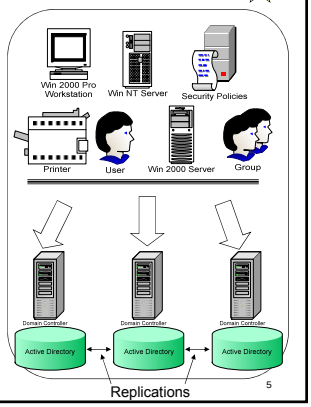
Domain	Shared folder
User Account	Computer
Group	Printer
Shared Drive	



4

Replication

- In a Windows 2003 network, you can create multiple domain controllers (DCs)
- Each DC stores a copy of the Active Directory
- Each DC replicates changes in its copy of Active Directory to other DCs.



5

Global catalog (GC)

- During AD installation, W2003 Server creates a Global Catalog on the 1st DC
- The Global Catalog stores:
  - ► Information about all objects in the initial DC
  - ► Partial information about objects in other domains (attributes needed for search).
- An index and partial replica of objects and attributes most often used in AD database

6

Global Catalog (GC)

- Common attributes stored in the GC: users' first and last names, logon names, email address
- GC is primarily for:
  1. Enabling users to find AD information from anywhere in the forest
  2. Providing authentication services when a user from another domain logs on with a User Principal Name (eg. john@east.contoso.com)
  3. Responding to directory lookup from application programs like Microsoft Exchange.

When a Global Catalog server is not available, the user can only logon to the local computer.

7

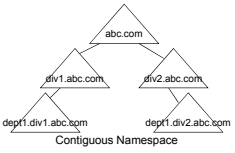
Namespace and DNS

- Domain Name Service (DNS): Service that performs name resolutions, i.e. conversions between IP addresses and domain names
- Name resolutions take place in a logical area of the network called Namespace
- A Namespace includes (1) the Active Directory, which contains named objects and (2) one or more DNS servers

8

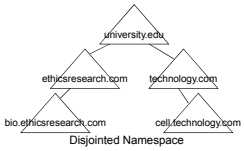
Types of namespaces

- **Contiguous namespace:** A namespace in which every child object contains the name of its parent object



Contiguous Namespace

- **Disjointed namespace:** A namespace in which the child object name does not resemble the name of its parent object

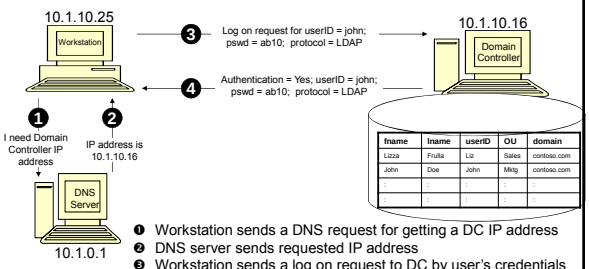


Disjointed Namespace

9

Active directory and DNS

- AD cooperates with DNS during logon process

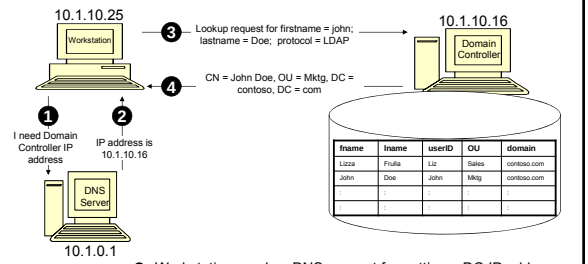


1. Workstation sends a DNS request for getting a DC IP address
2. DNS server sends requested IP address
3. Workstation sends a log on request to DC by user's credentials
4. DC sends back authentication response to workstation

10

Active directory and DNS

- AD cooperates with DNS in locating network resources and services

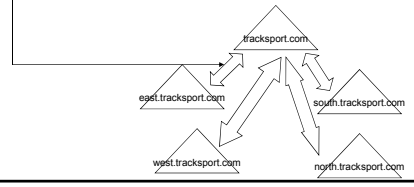


1. Workstation sends a DNS request for getting a DC IP address
2. DNS server sends requested IP address
3. Workstation sends the DC a request for locating a user account
4. DC sends back user's Unique Distinguish Name

11

Tree

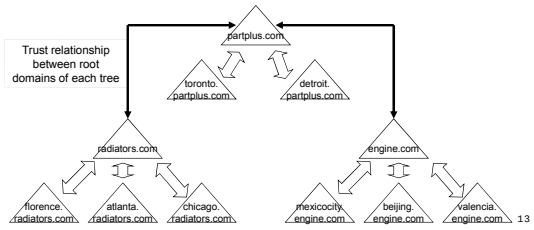
- A tree contains one or more domains and has the following characteristics:
  1) Domains are represented in a contiguous namespace
  2) Two-way trust relationships between domains (each domain can access other domain resources)
  3) Member domains use the same Schema and Global Catalog



12

Forest

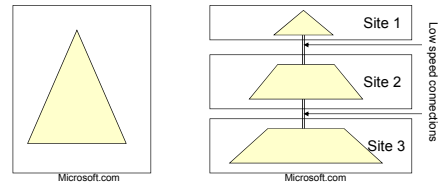
- Usually, a forest consists in more than one tree and has the following characteristics:
  1) The trees use a disjoined namespace
  2) All trees use the same Schema and Global Catalog



13

Site

- A TCP/IP concept used to reflect the physical design of the network. It has the following characteristics:
  1) Represents one or more IP subnets at the same location
  2) High speed connection in the same site
  3) Low speed connection between sites



Single domain with single site

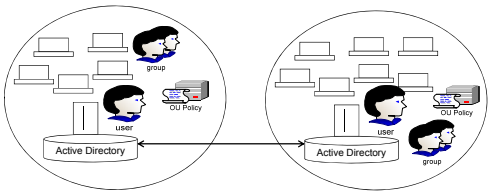
Single domain with multiple sites

14

Organizational Unit (OU)

Similar to having subfolders in a folder

- Grouping of related objects, such as user accounts, computers and printers for easier management.
  - OUs reflect functional structure of organization
  - Objects are grouped in an OU to be administered using the same group policy.



Manufacturing Division OU

Distribution Division OU

15

Summary Questions

1) In AD, a _____ stores information about all the objects in the initial DC and partial information about objects in other domains

   a) Forest
   b) Global Catalog
   c) Namespace
   d) Schema
   e) Site

2) Which of the following is a 128-bit number (that cannot change) assigned to an object?

   a) User Principal Name
   b) Universal Name
   c) Globally Unique Identifier

3) When combining domains in a tree, you have named the parent domain **univesity.com** while the two child domains added to this parent are named **computerscience.univesity.com** and **hystory.university.com**. Which of the following options have you selected for naming the domains?

   a) Disjointed
   b) Contiguous
   c) User Principal Name
   d) Globally Unique Identifier

16

Summary Questions

4) In Active Directory, a _____ represents the design of the AD database. It contains the definition of objects' attributes.

   a) Class
   b) Global Catalog
   c) Namespace
   d) Schema

5) Which of the following statements is/are true regarding a site?

   a) High speed connections are used in the site, whereas low speed connections are used between sites
   b) A site represents one or more subnets at the same physical location.
   c) All of the above

6) Trees in a forest use:

   a) Different Global catalogs
   b) Same schema
   c) Always use the same naming structure

7) A(n) _____ is a grouping of related objects, usually, based on the functional structure of the organization

   a) Site
   b) Organizational Unit
   c) tree

17