ACTIVEDIRECTORY

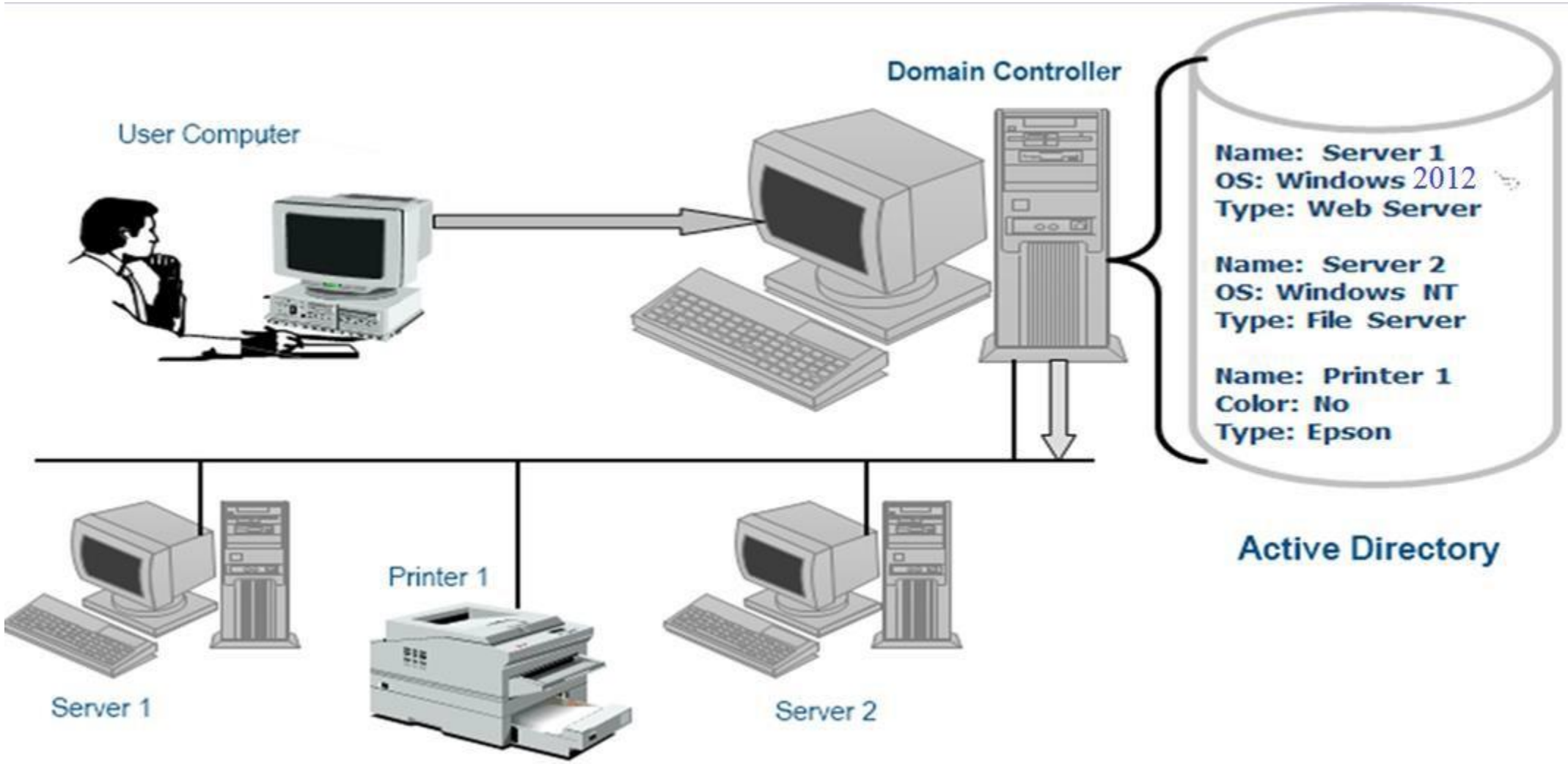
Nội dung

- Active Directory (AD) là gì
- Kiến trúc Active Directory
- Cài đặt Active Directory Domain Services (AD-DS)

Thư mục động (Active Directory)

- Active Directory là thành phần quan trọng của hệ điều hành máy chủ:
  - Active Directory (AD): là nơi lưu trữ thông tin tài nguyên mạng: User data, printers, servers, databases, groups, computers, and security policies… được tổ chức theo miền, cây, rừng.
  - Thông tin được sử dụng để truy xuất và quản lý tài nguyên trên mạng
  - Cung cấp một cách đặt tên nhất quán giúp mô tả, định vị, truy xuất và bảo mật tài nguyên mạng

Active Directory



Thuận lợi của Active Directory

- Ưu điểm Active Directory:
  - Đơn giản hóa quản lý bảo mật (Domain, OU)
  - Lưu trữ dự phòng thông tin bảo mật
  - Chính sách nhóm
  - Khả năng mở rộng
  - Ủy quyền quản trị

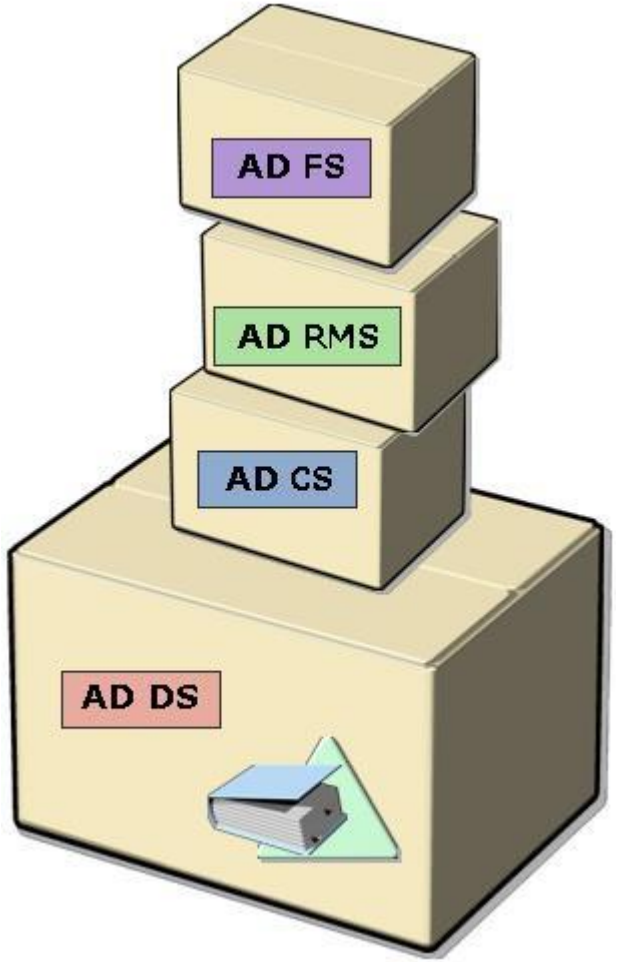
Active Directory Server Roles là gì?

Server Role	Mô tả
Active Directory Domain Services (AD DS)	Một thư mục tập trung quản lý và chứng thực cho người sử dụng và máy tính trong mạng Windows Server
Active Directory Lightweight Directory Services (AD LDS)	Một dịch vụ thư mục LDAP (Lightweight Directory Access Protocol) cung cấp một cơ chế nhằm hỗ trợ các ứng dụng directory-enabled (sử dụng thư mục để lưu trữ dữ liệu), mà không có yêu cầu triển khai miền, bộ điều khiển miền.
Active Directory Certificate Services (AD CS)	Một giải pháp được sử dụng để bảo vệ thông tin được lưu trữ trong các văn bản, tin nhắn, e-mail và các trang Web không được phép xem, sửa đổi, hoặc sử dụng
Active Directory Rights Management Services (AD RMS)	Là dịch vụ được dùng để kết hợp với các ứng dụng hỗ trợ AD RMS (AD RMS – enable application), nhằm bảo vệ dữ liệu quan trọng trước những đối tượng người dùng không được phép (unauthorized users).
Active Directory Federation Services (AD FS)	Là một dịch vụ cung cấp cơ chế đăng nhập - single sign- on (SSO), cho phép bạn đăng nhập chỉ một lần nhưng có thể dùng nhiều ứng dụng Web có quan hệ với nhau.

Active Directory

- Active Directory Domain Services (AD DS) là một dịch vụ trên WServer, sử dụng thông tin lưu trữ trong Active Directory để quản lý các đối tượng users, group, computer.
- Cung cấp thông tin về tài nguyên dựa vào thuộc tính của tài nguyên.
  - Tự phân tán đến các máy tính trên mạng.
  - Tự nhân bản: giúp ADDS tự bảo vệ, dễ truy xuất.
  - Có khả năng phân tán -> tăng khả năng lưu trữ
- Gồm nhiều phần: miền, cấu hình, lược đồ

AD DS Integration with Other Active Directory Server Roles

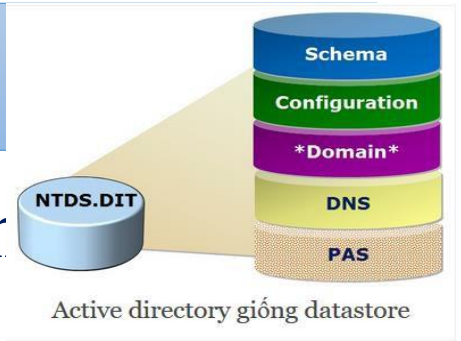


- AD DS là nền tảng cho một mạng chức năng
- Hầu hết các vai trò máy chủ phụ thuộc vào AD DS để cung cấp cho người sử dụng và nguồn tài nguyên thông tin cho các vai trò máy chủ khác
- AD DS cũng cung cấp dịch vụ xác thực và ủy quyền

Kiến trúc Active Directory

- Kiến trúc
- Đối tượng AD (Active Directory Objects)
- Lược đồ AD (Active Directory Schema)
- Các thành phần AD (Active Directory Components – cấu trúc luận lý và cấu trúc vật lý)

Kiến trúc Active Directory

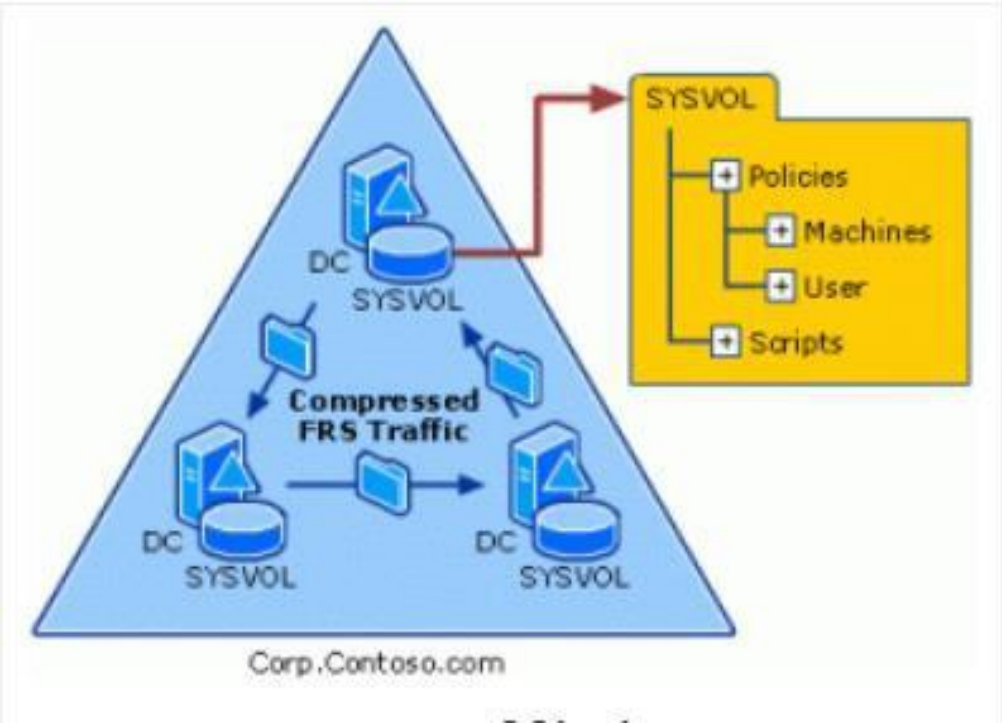


Active directory giống datastore

- Active Directory như một Datastore có 2 thành ph
  - NTDS.DIT có 5 thành phần
    - **Domain NC**: chứa các đối tượng như user, computer, OU….
    - **Schema**: là nơi lưu trữ các định nghĩa về từng thuộc tính trên mỗi đối tượng
    - **Configuration**: chứa toàn bộ các cấu hình của ***Active Directory***
    - **DNS**: lưu thông tin cấu hình DNS
    - **Global Catalog** (PAS): đảm nhiệm chức năng chứng thực (**authentication**) cho hệ thống Active Directory. Máy chủ quản trị miền nào (Domain controller) lưu trữ Global Catalog thì được gọi là Global Catalog Server.

Kiến trúc Active Directory

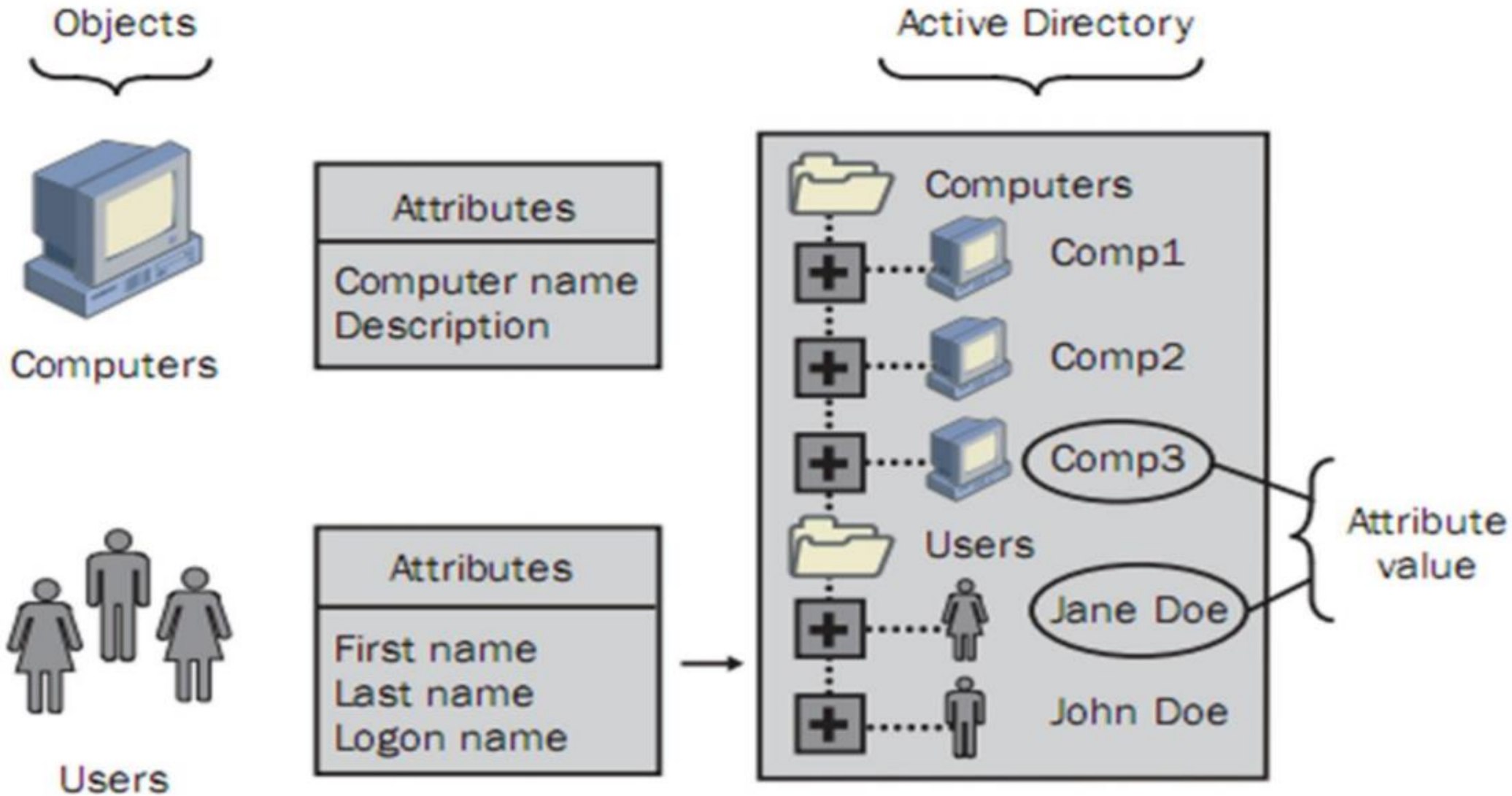
- Active Directory như một Datastore có 2 thành phần
  - **SYSVOL:** là một thư mục chứa các chính sách dành cho các đối tượng người dùng hoặc máy tính và các đoạn script quan trọng khác.



Đối tượng AD

- Thông tin users, máy in, server, database, groups, computers và security policies
- Mỗi object có những thuộc tính riêng đặc trưng cho object đó (ví dụ như object user có các thuộc tính liên quan như First Name, Last Name, Logon Name, …)
- Một số object đặc biệt bao gồm nhiều object khác bên trong được gọi là các “container”, (ví dụ như domain là một container bao gồm nhiều user và computer account).

Đối tượng AD


Objects
Active Directory
Computers
Attributes
Computer name
Description
Computers
Comp1
Comp2
Comp3
Users
Jane Doe
John Doe
Attribute value
Users
Attributes
First name
Last name
Logon name

Các quy ước đặt tên trong AD

- Mỗi đối tượng trong Active Directory được nhận biết thông qua một tên
- Active Directory hỗ trợ các quy ước đặt tên bao gồm:
  - Distinguished Name (DN)
  - Globally Unique Identifier (GUID)
  - Relative Distinguished Name (RDN)
  - User Principal Name (UPN)

Các quy ước đặt tên trong AD-DN

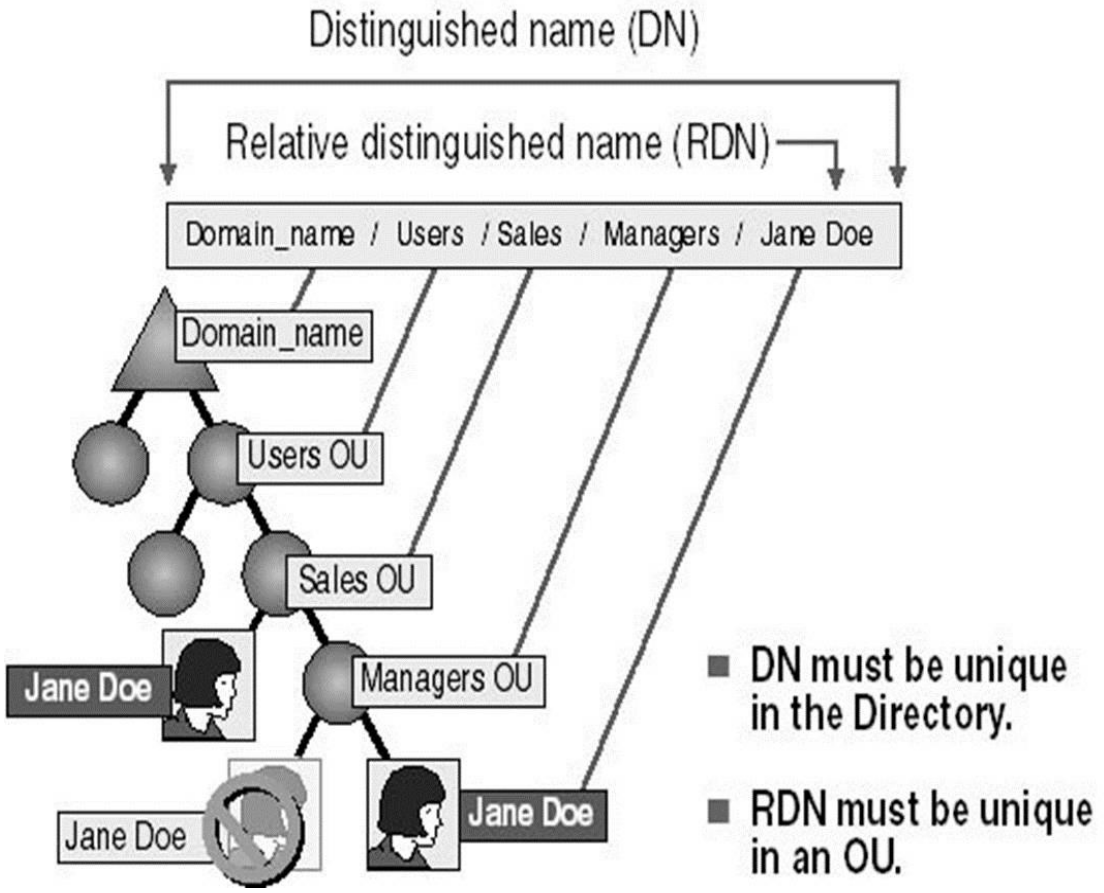
- Distinguished Name (DN)
  - Mỗi đối tượng trong Active Directory sẽ có một tên duy nhất dựa trên giao thức **LDAP** (Lightweight Directory Access Protocol)
  - DN chứa đầy đủ thông tin về đối tượng bao gồm:
    - Tên của miền nơi lưu trữ đối tượng
    - Đường dẫn đầy đủ tới đối tượng
  - Thí dụ sau đây chỉ ra DN của người dùng David Beckham trong Cty abc (abc.com) và thuộc phòng Development (OU=Dev):
    /DC=com/DC=abc/OU=dev/CN=Users/CN=David Beckham
    DC: Domain Component Name
    OU: Organizational Unit Name
    CN: Common Name

Các quy ước đặt tên trong AD-GUID

- Globally Unique Indentifier (GUID)
  - Các GUID là các số 128 bit duy nhất được gán cho đối tượng tại thời điểm nó được tạo.
  - GUID không bao giờ thay đổi ngay cả khi đối tượng được đổi tên (DN) hay di chuyển.
  - Tương tự như một SID (Security Identifiers) trong Windows NT nhưng:
    - SID được tạo bên trong một miền là duy nhất trong miền đó
    - GUID là duy nhất trên tất cả các miền trong một rừng
  - GUID giống như số CMNN của một người nào đó

Các quy ước đặt tên trong AD-RDN

- ADDS hỗ trợ truy vấn thông qua thuộc tính của một đối tượng, do đó có thể xác định được đối tượng ngay cả khi không biết DN.
- RDN của một đối tượng là thuộc tính của đối tượng đó



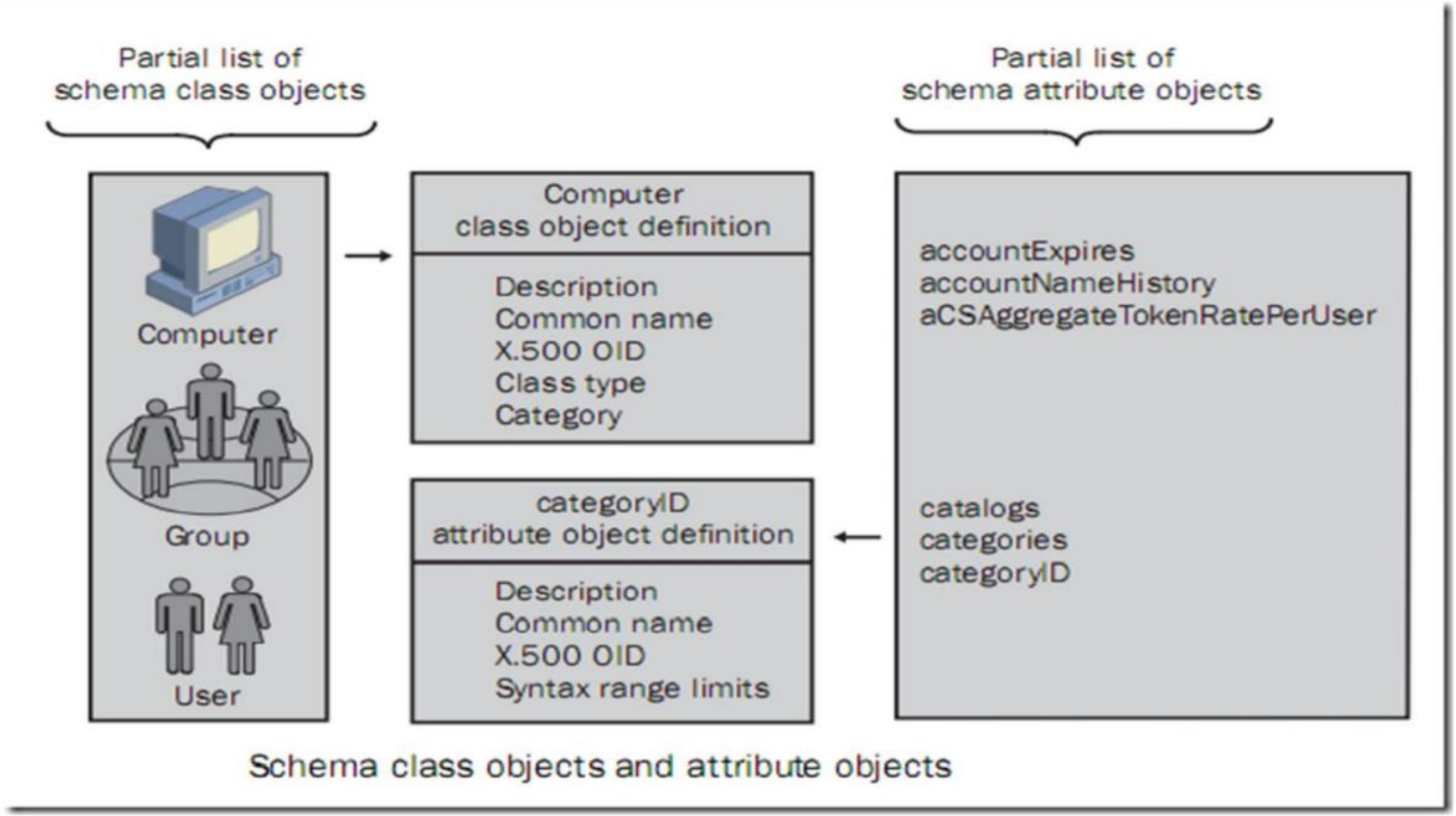
Các quy ước đặt tên trong AD-UPN

- User Principal Name (UPN)
- Là tên thân thiện của đối tượng người dùng.
- Nó là sự kết hợp giữa một tên ngắn của đối tượng và tên
- DNS của Domain nơi lưu giữ đối tượng.
- Tên ngắn thường là tên đăng nhập (logon) của người dùng.
  - Ví dụ: đối với người dùng Lam Chi Nguyen có tên đăng nhập là lcnguyen, thì UPN sẽ là: lcnguyen@abc.com

Lược đồ AD

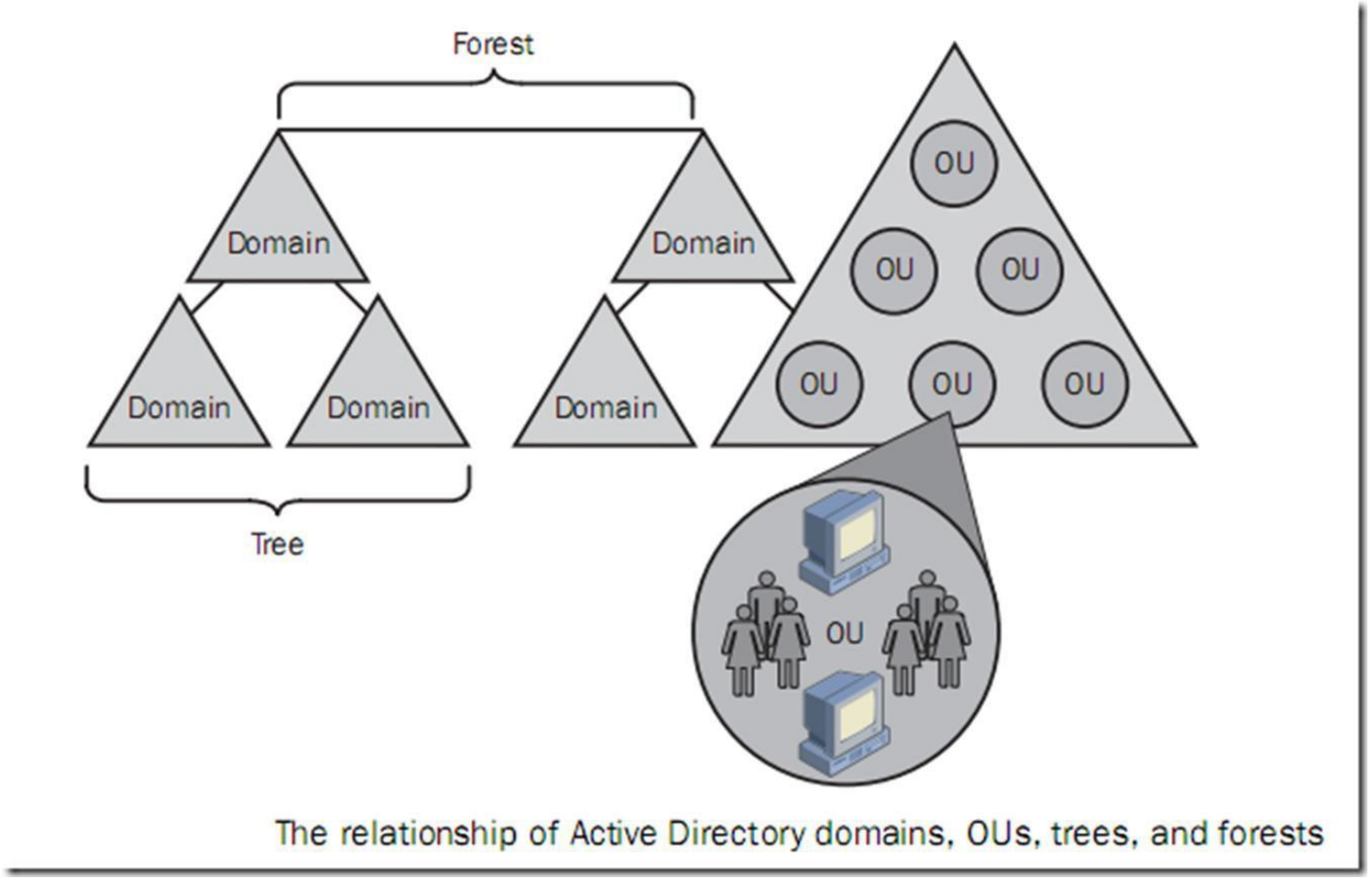
- Chứa những định nghĩa về các đối tượng khác nhau được lưu trữ trong AD.
- Các định nghĩa được lưu trữ như đối tượng trong AD.
- Lược đồ là duy nhất trong một rừng và được tạo ra trong quá trình cài đặt Domain Controller đầu tiên của rừng.
- Schema được định nghĩa gồm 2 loại object là Schema Class Objects và Schema Attribute Objects.
  - Schema Class có chức năng như một template cho việc tạo mới các đối tượng trong AD.
  - Schema Attribute định nghĩa các Schema Class tương ứng với nó.

Lược đồ AD


Partial list of
schema class objects
Partial list of
schema attribute objects
Computer
Group
User
Computer
class object definition
Description
Common name
X.500 OID
Class type
Category
categoryID
attribute object definition
Description
Common name
X.500 OID
Syntax range limits
accountExpires
accountNameHistory
aCSAggregateTokenRatePerUser
catalogs
categories
categoryID
Schema class objects and attribute objects

Cấu trúc luận lý (Logical Structure)

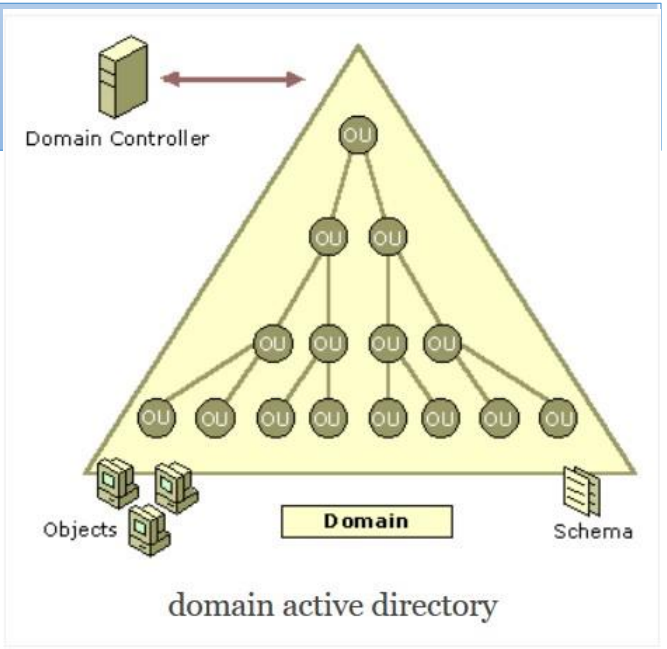
- Được ánh xạ thông qua mô hình domains, OUs, trees và forest



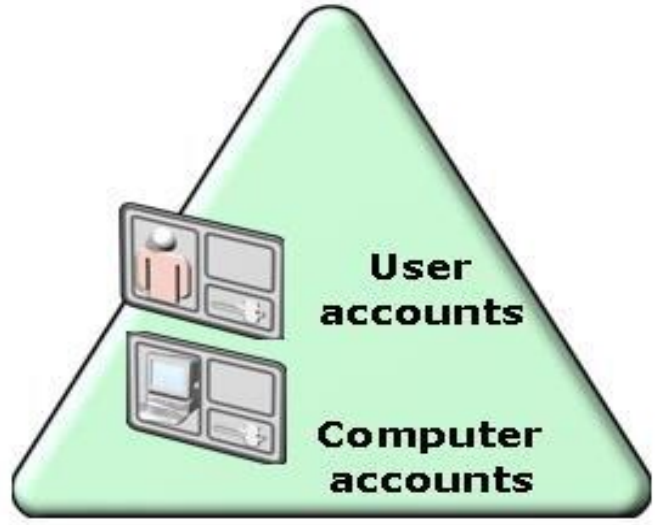
The relationship of Active Directory domains, OUs, trees, and forests

Miền (Domain)

- Trong một miền thì phải có ít nhất là một máy chủ quản lý miền (**Domain Controller**)
- Nó là sự tập hợp các máy tính được định nghĩa bởi người quản trị.
- Tất cả các máy tính trong miền dùng chung một cơ sở dữ liệu Active Directory chia sẻ
- Mục đích chính của miền là phục vụ như một ranh giới bảo mật trong mạng Windows Server.
- Các máy chủ trong cùng một miền sẽ đồng bộ với nhau về các đối tượng trong miền đó (Domain Name Context)

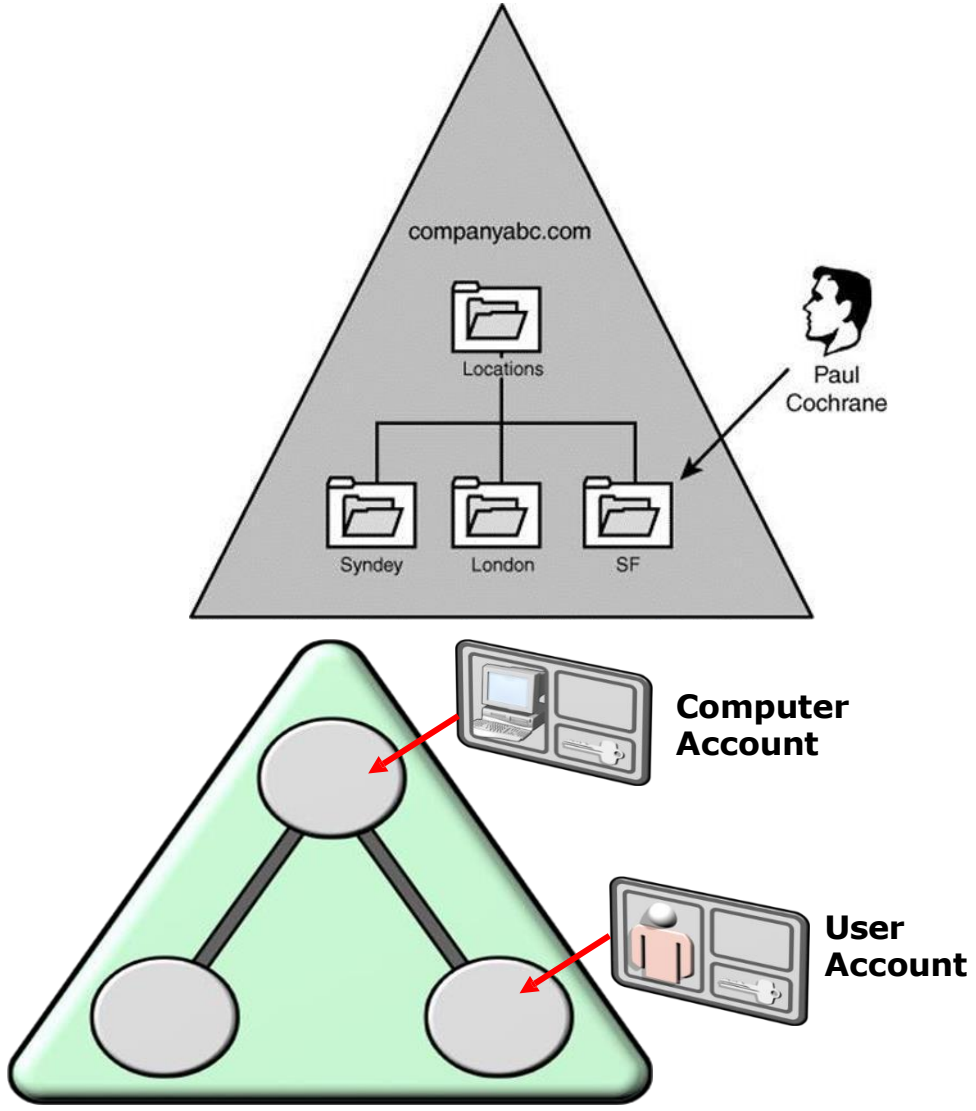


domain active directory



Đơn vị tổ chức OU (Organization Unit – OUs)

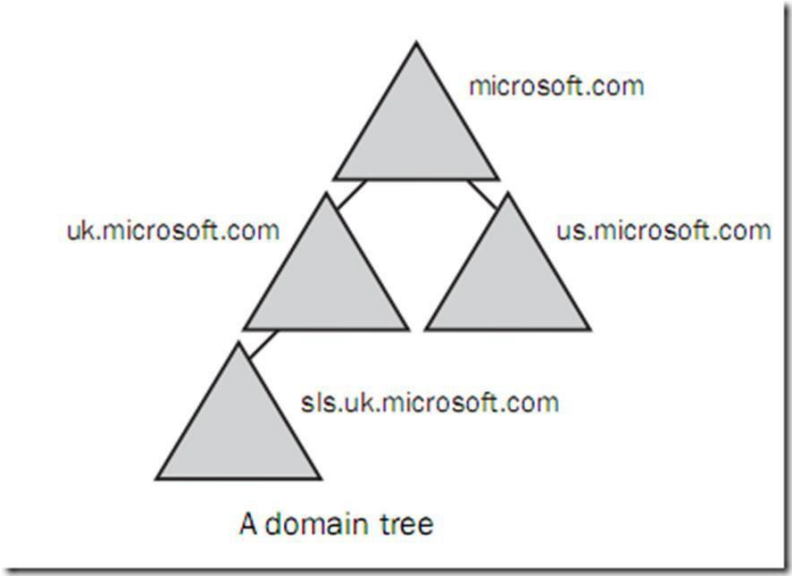
- Trong miền, các đối tượng được sắp xếp và tổ chức bằng cách sử dụng các OU.
- Nó chứa các đối tượng như người dùng, máy tính, máy in, nhóm và OUs khác.
- OU giúp cho việc phân loại và tổ chức các đối tượng một cách hợp lý như ý của bạn



Cây (Tree)

Là một nhóm của một hay nhiều domain, mà các domain này chia sẻ một không gian tên liền kề và cấu trúc đặt tên có thứ bậc.

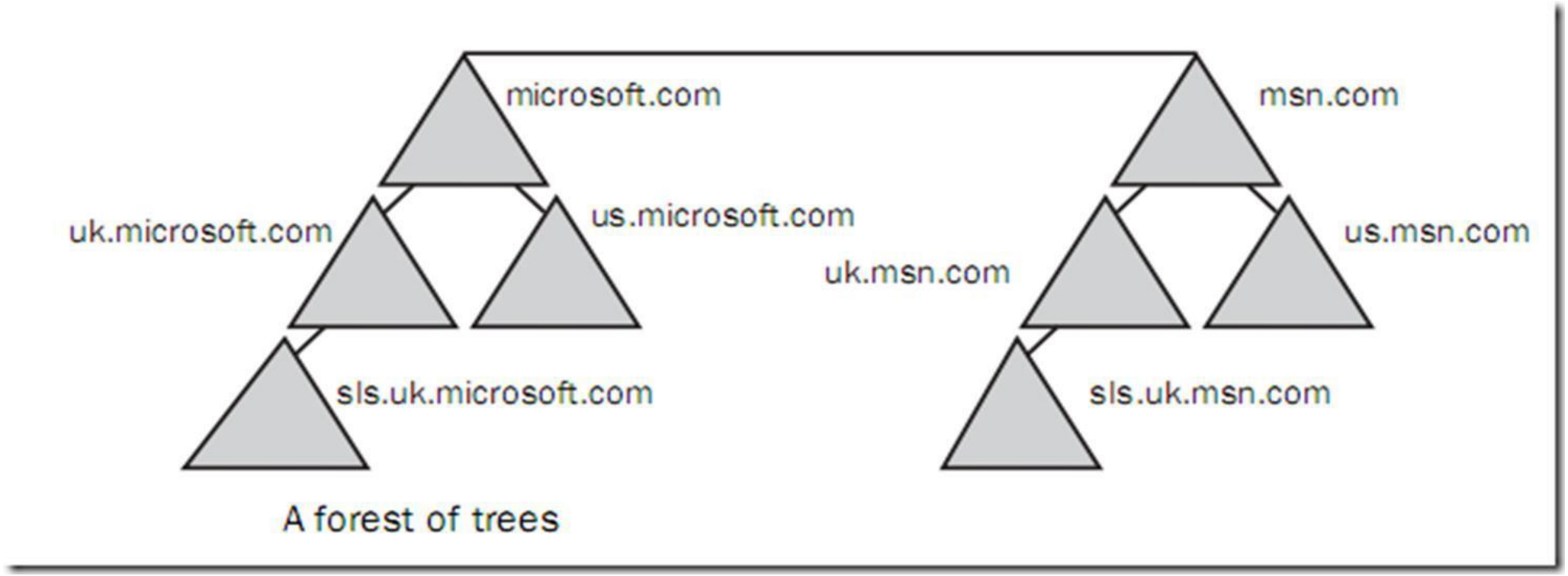
- Các đặc tính của cây:
  - Theo chuẩn DNS
  - Các Domain trong cây chia sẻ chung: Common schema và Global catalog



Những miền có sử dụng chung tên gốc hay tên miền không bị gián đoạn

Rừng (forest)

- **Forest:** Là tập hợp của nhiều **tree** có quan hệ với nhau
- Các domain trees trong forest là độc lập với nhau về tổ chức



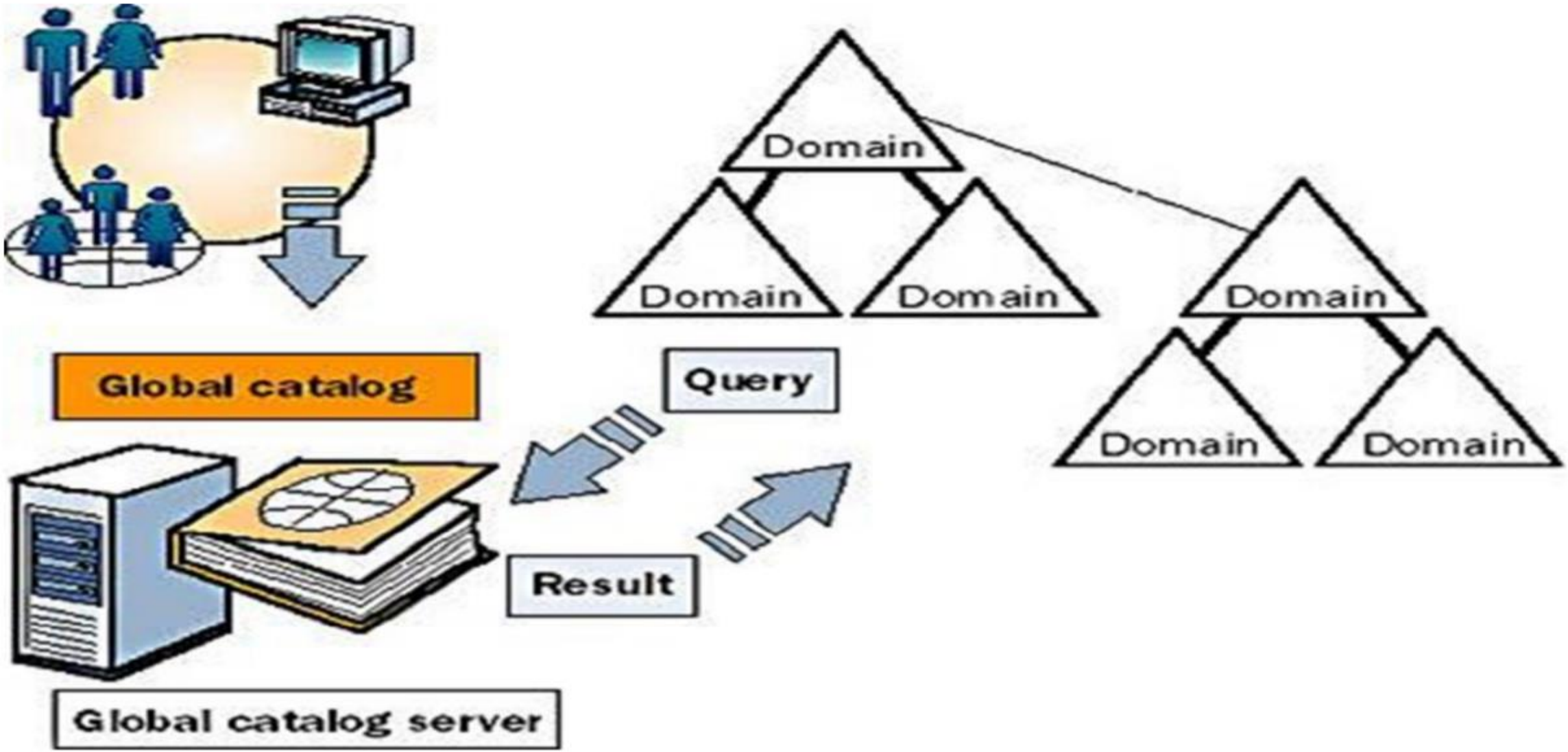
Rừng (forest)

- Một forest phải đảm bảo thoả các đặc tính sau
  - Toàn bộ domain trong forest phải có 1 schema chia sẻ chung
  - Các domain trong forest phải có 1 global catalog chia sẻ chung
  - Các domain trong forest phải có mối quan hệ trust 2 chiều với nhau
  - Các tree trong 1 forest phải có cấu trúc tên(domain name) khác nhau
  - Các domain trong forest hoạt động độc lập với nhau, tuy nhiên hoạt động của forest là hoạt động của toàn bộ hệ thống tổ chức doanh nghiệp.

Danh mục toàn cục (Global Catalog)

- Global catalog là trung tâm lưu giữ các thông tin của các đối tượng trong Active directory
- Nhưng thông tin (thuộc tính của đối tượng) được lưu trữ trong Global catalog thường xuyên được sử dụng cho hoạt động tìm kiếm và định vị các đối tượng trong AD
- Global catalog được tạo ra trong Domain Controller đầu tiên của Forest -> Global Catalog Server

Danh mục toàn cục (Global Catalog)

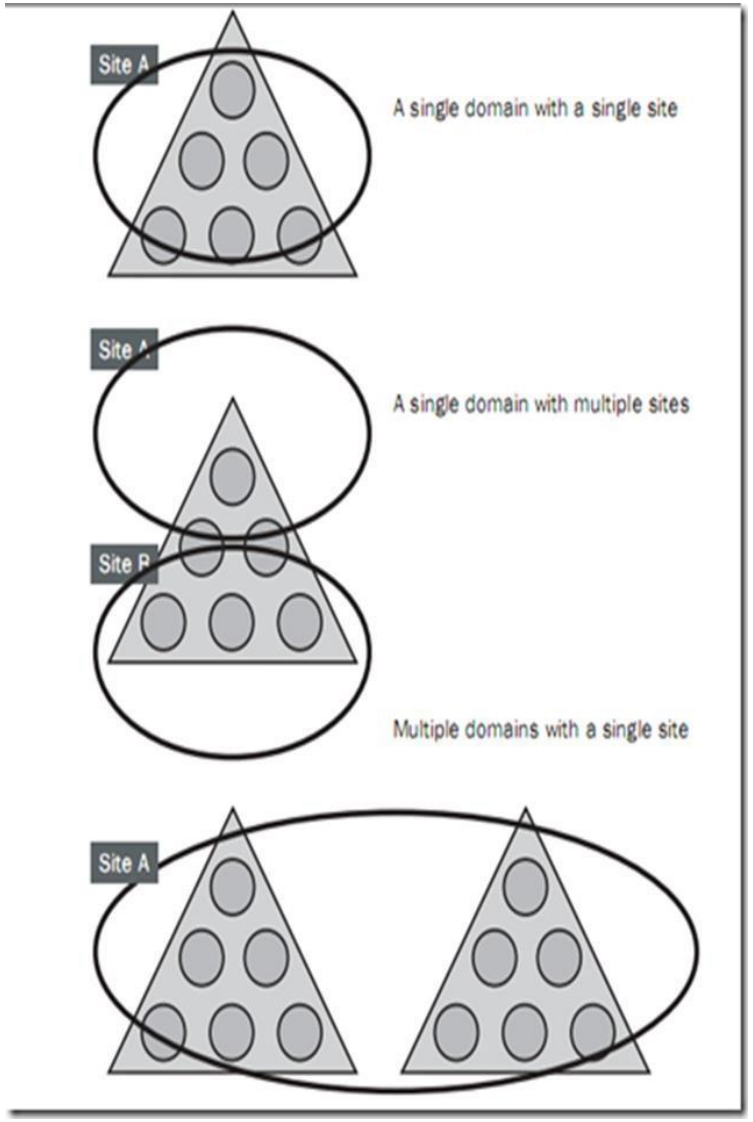


Cấu trúc vật lý của AD (Physical Structure)

- Cấu trúc vật lý và cấu trúc logic là hoàn toàn tách biệt
- Cấu trúc vật lý được sử dụng để tổ chức việc trao đổi trên mạng, trong khi cấu trúc logic dùng để tổ chức tài nguyên trên mạng.
- Cấu trúc vật lý của AD gồm:
  - Sites
  - Domain Controllers

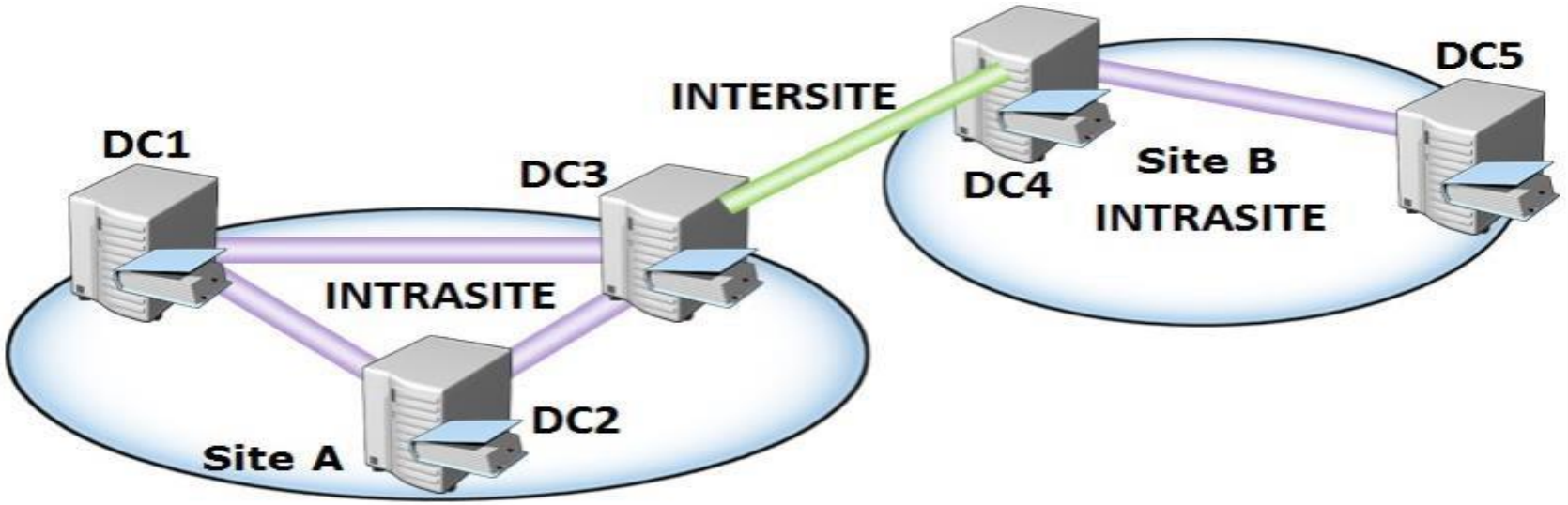
Sites

- Là một thuật ngữ được dùng đến khi nói về vị trí địa lý của các domain trong hệ thống.
- Một site là một sự kết hợp của một hoặc nhiều subnets IP được kết nối với tốc độ cao
- Các Sites được định nghĩa để tối ưu hoá việc truy xuất và nhân bản Active Directory.
- Mục đích chính của việc định nghĩa các sites là:
  - Để đảm bảo chắc chắn kết nối tốc độ cao giữa các domain controllers
  - Để tối ưu hoá băng thông giữa các site



Sites

Khái niệm này thường được chia theo vùng, ví dụ công ty của bạn có 2 chi nhánh, một tại Hà Nội và một tại Hồ Chí Minh. Khái niệm Site ở đây được hiểu là khi các máy trong đó thuộc về cùng một subnet địa chỉ IP. Các máy chủ trong cùng một subnet thì được gọi là Intrasite, còn các máy chủ nằm khác subnet thì được gọi là Intersite.



intrasite intersite active directory

Bộ điều khiển miền (Domain Controllers)

- Một domain controller (DC) là một máy chạy Windows Server và nó chứa một bản sao của Active directory.
- Các chức năng của Domain Controller:
  - Duy trì một bản sao CSDL của active directory
  - Các DC trong một domain tự động nhân bản tất cả các đối tượng trong domain tới mỗi DC.
  - Duy trì thông tin của các đối tượng trong Active Directory
  - Cung cấp khả năng chịu lỗi trong môi trường đa DC.
  - Quản lý và hỗ trợ người sử dụng trong việc tìm kiếm thông tin trên AD

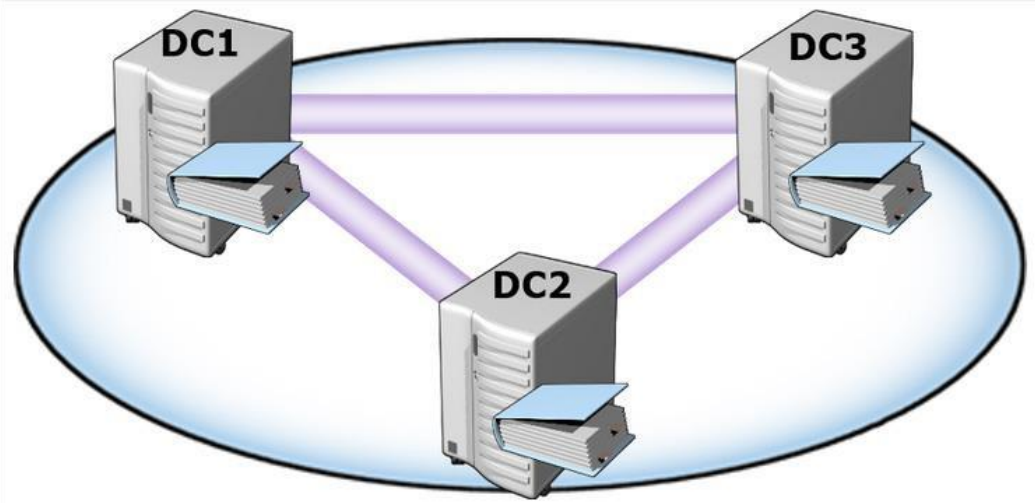
Nhân bản (Replication) trong AD

- Nhằm bảo đảm rằng những thay đổi trên bất kỳ Domain Controller nào cũng được phản ánh tới các DC khác trong miền.
- Những thông tin trong Active Directory gồm:
  - Thông tin lược đồ.
  - Thông tin cấu hình.
  - Thông tin miền.
  - Thông tin phần mềm ứng dụng.

Ví dụ: trên DC thứ nhất, bạn được phép truy cập vào tài nguyên A, trong khi theo máy chủ DC thứ 2, bạn lại không có được quyền này???

Nhân bản (Replication)

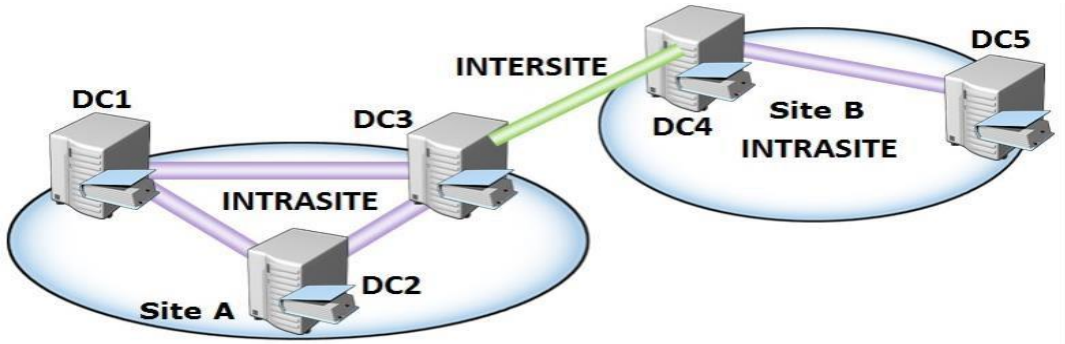
- Một hệ thống thì phải có sự nhất quán rõ ràng, từ các đối tượng, cho tới các chính sách thực thi,
- Cần phải có một sự đồng bộ giữa các các máy chủ quản lý về đối tượng, chính sách .v.v,



Replication Active Directory

Nhân bản (Replication)

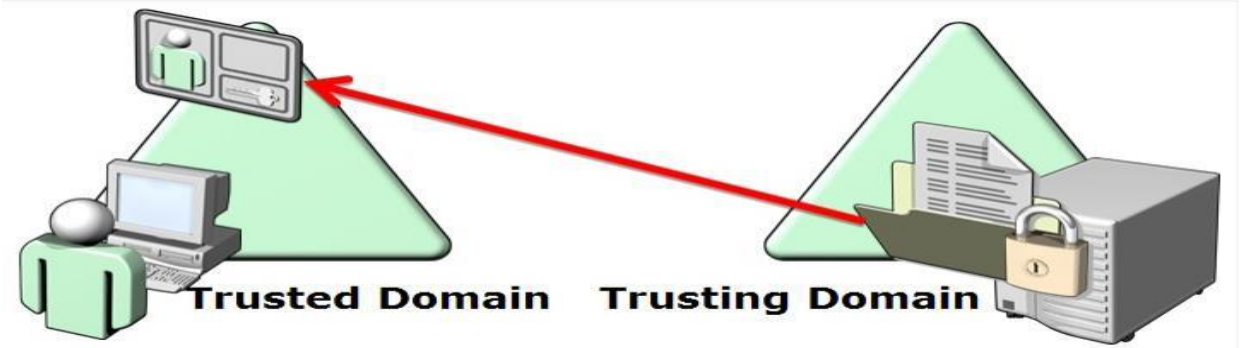
- Nhân bản bên trong Site là nhanh và tin cậy.
- Nhân bản giữa các Sites
  - Sử dụng thông tin kết nối mạng tạo ra kết nối đối tượng, điều này cung cấp tính chịu lỗi và khả năng phục hồi.
  - Việc nhân bản sẽ có hiệu quả cao nếu các lịch biểu nhân bản được tối ưu, ví dụ lên lịch nhân bản khi lưu lượng mạng ít.
- Quá trình nhân bản kết thúc khi tất cả các bộ điều khiển miền đã được cập nhật.



intrasite intersite active directory

Trust Relationships

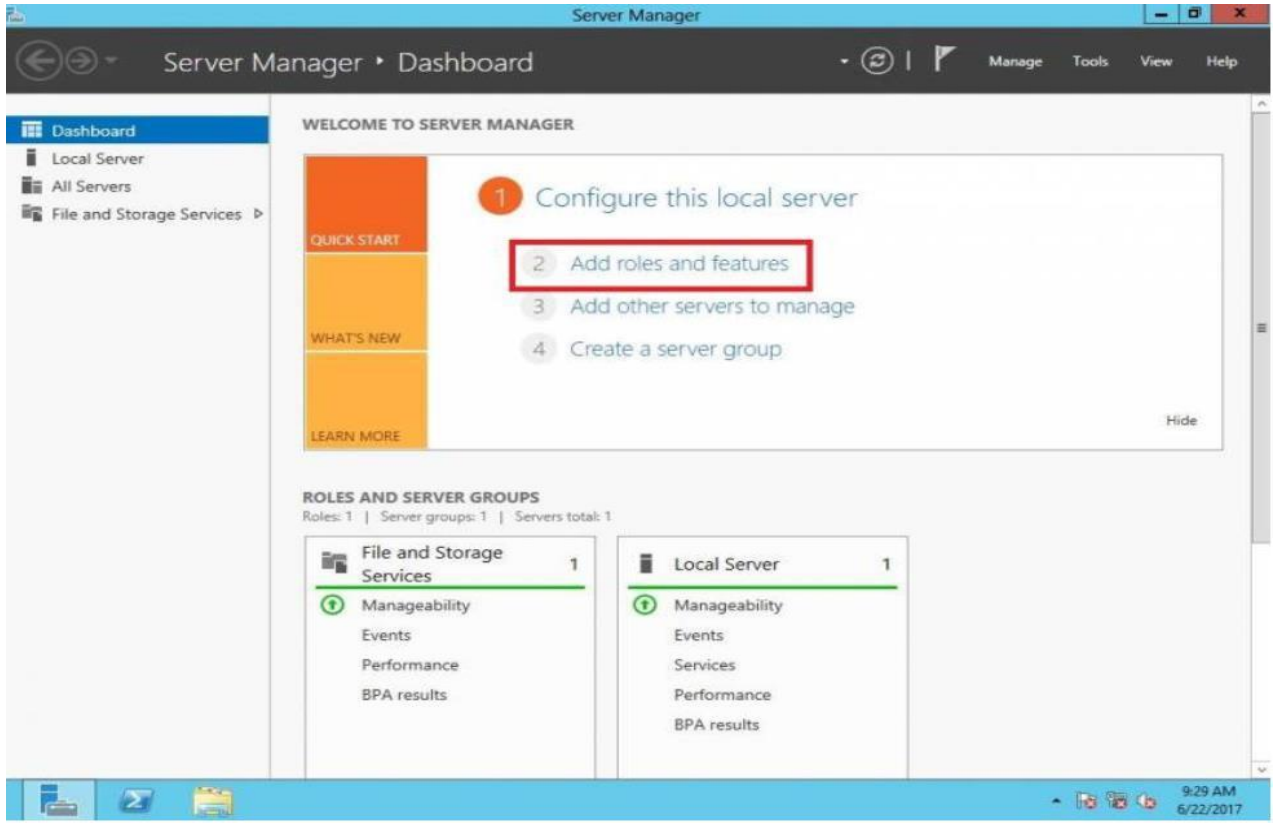
- **Trust Relationships:**
  - Domain A, khi tin cậy một domain B, quản trị viên domain A có thể cho phép người dùng bên domain B, truy cập vào tài nguyên của mình.
  - Tuy nhiên, người dùng ở domain A, thậm chí ngay cả quản trị viên domain A cũng không thể truy cập vào tài nguyên của B, do không được domain B tin tưởng.
  - Điều này chỉ có thể xảy ra, khi quản trị viên từ domain B cũng có một động thái tương tự.



trust relation ship active directory

Cài đặt Active Directory trên Windows Server 2012

- Cấu hình IP tĩnh cho máy
- Đặt tên máy: serverxx (server41)
- Tên miền của đơn vị: domainXX.com (domain41.com)
- Vào Server Manager, chọn Add roles and features:



Cài đặt Active Directory trên Windows Server 2012

- Ấn Next để giữ nguyên các cài đặt mặc định. Đến Select server roles -> Chọn Active Directory Domain Services (AD DS) và DNS Server:
- Xem thêm tài liệu