

## NỘI DUNG KIỂM TRA VÀ THI CUỐI KỲ

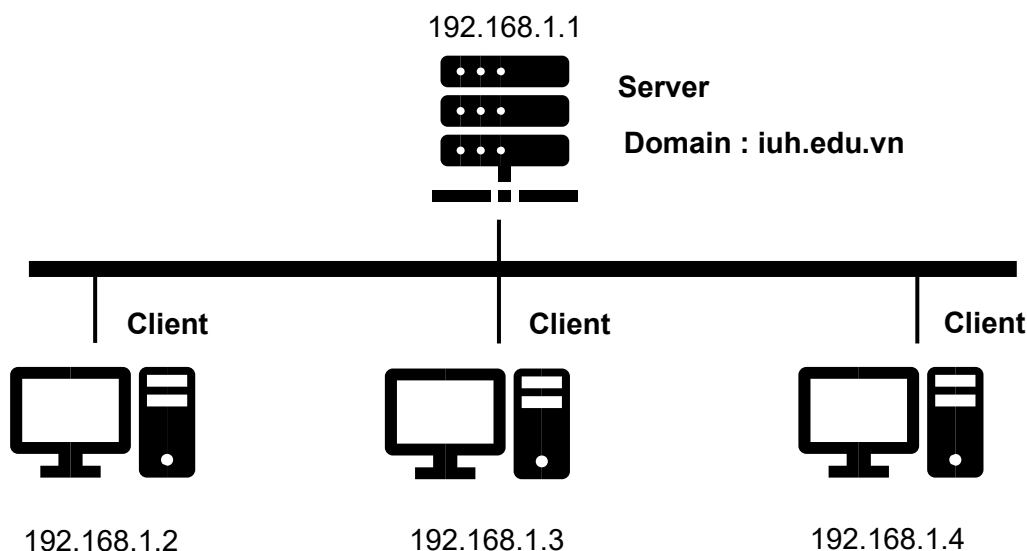
**CÂU 1:** Vận dụng kiến thức về quản trị hệ thống để xác định các giải pháp liên quan đến:

### Hiện thực:

Vận dụng được kiến thức quản trị hệ thống và đưa ra được giải pháp quản trị phù hợp theo yêu cầu của hệ thống mạng. Cài đặt và triển khai được giải pháp

### - Quản trị domain

**Mô hình:**



### **Vận dụng kiến thức về quản trị domain:**

Để đưa ra giải pháp quản trị phù hợp cho hệ thống mạng về quản trị domain, có thể áp dụng các phương pháp và công cụ quản trị hệ thống sau đây:

1. Thiết lập và quản lý máy chủ domain controller: Domain controller là máy chủ quản lý danh sách người dùng, nhóm và chính sách quyền truy cập trong mạng domain. Cần đảm bảo rằng máy chủ domain controller được cài đặt và cấu hình đúng, đảm bảo tính bảo mật và khả năng sẵn sàng cao.
2. Quản lý người dùng và nhóm: Xác định và tạo người dùng, nhóm và quyền truy cập tương ứng với từng người dùng trong domain. Điều này giúp tăng tính bảo mật, kiểm soát quyền truy cập và dễ dàng quản lý tài nguyên trong mạng.
3. Cấu hình chính sách bảo mật: Sử dụng công cụ Group Policy để thiết lập các chính sách bảo mật trên mạng domain. Các chính sách này có thể bao gồm mật khẩu phức tạp, khóa tài khoản sau một số lần đăng nhập không thành công, giới hạn quyền truy cập vào tài nguyên và hạn chế các hoạt động không an toàn.
4. Quản lý phân phối phần mềm cấp phát tài nguyên: Sử dụng tính năng quản lý phân phối phần mềm trong mạng domain để tự động triển khai và cập nhật phần mềm cho các máy tính trong mạng. Điều này giúp đơn giản hóa quá trình cài đặt và bảo trì phần mềm trong toàn bộ hệ thống.
5. Giám sát và bảo trì hệ thống: Đảm bảo rằng hệ thống domain đang hoạt động một cách ổn định và bảo mật. Thực hiện việc giám sát hệ thống, đảm bảo sự sẵn sàng của máy chủ domain

controller và các dịch vụ liên quan. Thực hiện sao lưu dữ liệu định kỳ và xây dựng kế hoạch khắc phục sự cố.

6. Đào tạo người dùng và quản trị viên: Đảm bảo rằng người dùng và quản trị viên trong hệ thống có đủ kiến thức và kỹ năng để sử dụng các tính năng và công cụ quản trị domain.

**c. Xác định các giải pháp thực hiện (Thực hiện trên Windows Server 2019) (Đây là các bước thực hiện; nếu đề có cho chi tiết thì làm chi tiết như VD file server; kiểu cụ thể hơn như User là ai, Máy DC là máy nào, Nhóm nào,.....):**

➤ **Thiết lập và quản lý máy chủ domain controller (Là cái máy đề cho hoặc trong mô hình của mình):**

- Tiến hành đặt IP tĩnh cho máy được chọn làm domain controller, trỏ DNS về chính Server được chọn làm máy chủ domain
- Trên máy Server được chọn làm domain. Tiến hành xây dựng Domain controller □ Cài đặt dịch vụ AD-DS (Active Directory Domain Services)
  - Tiến hành thăng cấp máy chủ thành domain controller (Promote this server to a domain controller)
  - Cấu hình triển khai với các bước để thiết lập domain
- Tiến hành đặt địa chỉ IP, trỏ DNS các máy client vào DNS máy domain controller và tiến hành gia nhập các máy client vào domain vừa được tạo

➤ **Quản lý người dùng và nhóm (Là cái người dùng hoặc nhóm hoặc OU đề cho làm như File Server):**

- Xác định các người dùng và nhóm và quyền truy cập tương ứng trong domain
- Tiến hành xác định các OU(Organization Unit), các nhóm người dùng (Group), người dùng (User) và tạo các OU, Group, User tương ứng
  - Vào Active Directory User and Computer
  - Chọn Domain và tạo các OU, Group, User tương ứng
  - Áp dụng các chính sách bảo mật đối với từng đối tượng người dùng và nhóm người dùng
- Tiến hành gia nhập các User vào Group; các Group vào các OU tương ứng

➤ **Cấu hình chính sách bảo mật (Đây là bước thực hiện. Còn giải pháp là: User A có quyền truy cập DC; Group B không có quyền với thư mục,.....(đề bài cho). Làm kiểu như File server):**

- Sử dụng công cụ Group Policy để cấu hình các chính sách bảo mật; GPO(Group Policy Object) có 2 chính sách là Default Domain Controller Policy (Áp dụng cho DC) và Default Domain Policy (Áp dụng cho toàn hệ thống), cho phép cài đặt các chính sách như ( Cho phép User đăng nhập vào DC, Cài đặt chính sách mật khẩu đối với việc quản lý người dùng, Cho phép hoặc không cho phép User thay đổi cài đặt, .... )
- Để cho phép User đăng nhập vào máy DC:
  - Default Domain Controllers Policy →Edit→Computer Configuration →Policies →Windows Settings →Security →User Right Assignment →Allow log on locally → Add User →Apply và chạy lệnh gpupdate /force trong cửa sổ Run để tiến hành cập nhật chính sách
- Để hiệu chỉnh các chính sách mật khẩu:
  - Default Domain Policy →Edit → Computer Configuration →Policies →Windows Settings →Security →Password Policy → Thực hiện các

cài đặt tương ứng → Chạy lệnh gpupdate /force trong cửa sổ Run để tiến hành cập nhật chính sách

➤ **Quản lý phân phối phần mềm và cấp phát tài nguyên cho người dùng:**

- (Cài thư mục này được lưu trữ bao nhiêu; cấm các file nào, OU nào link... đề nếu cho)
- Thực hiện phân phối phần mềm bằng Deploy Software
  - Tạo GPO mới mang tên tương ứng
  - Edit → User Configuration → Policies → Software Settings → Software Install → New → Package → Tiến hành chọn đường dẫn lưu trữ phần mềm (Lưu ý phải là đường dẫn mạng (bằng cách chia sẻ file cài đặt qua mạng)) → Thực hiện các cấu hình tương ứng
  - Link từ GPO mới được tạo sang các OU mong muốn
  - Cập nhật chính sách bằng lệnh gpupdate /force trong cửa sổ Run
  - Các User trong OU khi đăng nhập các phần mềm tự động cài đặt ○ Thực hiện cấp phát tài nguyên bằng File Server Resource Manager: □ Giới hạn dung lượng lưu trữ (Disk Quota)
    - File Server Resource Manager → Quota Management → Quotas → Create Quota → Thực hiện các cấu hình phù hợp với yêu cầu tương ứng
  - Giới hạn không cho phép chép các file không được phép
    - File Server Resource Manager → File Screening Management → File Group → Create File Group → Thực hiện các cài đặt phù hợp
    - Áp dụng các cài đặt vào ổ đĩa/folder → File Server Resource Manager → File Screening Management → File Screen → Create File Screen.. → Custom Properties → Chọn File Group vừa được cài đặt → Save/OK

➤ **Giám sát và bảo trì hệ thống**

➤ **Đào tạo người dùng và quản trị viên:**

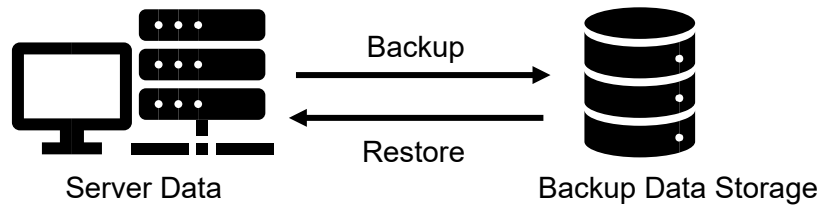
**d. Triển khai hệ thống ( Các bước thực hiện )**

Các bước như **phần c** hoặc nếu làm được làm giống File Server

=

## **Backup hệ thống, Restore hệ thống**

### **a. Xây dựng mô hình mạng và chuẩn bị máy ảo.**



\* **Backup Data Storage** có thể là một ổ đĩa/Thư mục trong chính Server hoặc là một nơi lưu trữ dữ liệu chuyên biệt ở bên ngoài và kết nối với Server bằng đường mạng

### **b. Vận dụng kiến thức về Backup hệ thống (System Backup), Restore Hệ thống (System Restore) .**

- ✦ Sao lưu hệ thống (System Backup) là việc tạo ra các bản sao của dữ liệu gốc và lưu trữ chúng ở một nơi an toàn. Khi hệ thống gặp sự cố, bạn có thể sử dụng các bản sao lưu để phục hồi lại dữ liệu. Việc này giúp tăng khả năng chịu lỗi của hệ thống và bảo vệ dữ liệu quan trọng của bạn.
- ✦ Phục hồi hệ thống (System Restore) là việc sử dụng các bản sao lưu để khôi phục lại dữ liệu và cài đặt của hệ thống về trạng thái trước đó. Việc này giúp người dùng có thể khắc phục các sự cố phần cứng, lỗi phần mềm hoặc các vấn đề khác mà có thể gây ra mất mát dữ liệu.
- Trong quản trị và bảo trì hệ thống, việc sao lưu hệ thống / Phục hồi hệ thống đóng vai trò quan trọng trong việc đảm bảo an toàn và tính sẵn sàng của dữ liệu. Ngăn ngừa mất mát dữ liệu do sự cố phần cứng, lỗi phần mềm hoặc các vấn đề khác, người dùng có thể khôi phục lại hệ thống về trạng thái hoạt động bình thường sau khi gặp sự cố. Ngoài ra, việc sao lưu hệ thống còn giúp quản trị viên có thể khôi phục lại hệ thống về trạng thái trước đó trong trường hợp cần thiết.

### **c. Xác định các giải pháp thực hiện (Thực hiện trên Windows Server 2019).**

- Xác định thư mục/Ổ đĩa cần backup ( C:\ ; D:\ .... Gì đó)
- Xác định nơi dùng để lưu trữ là máy (ABC gì đó) hoặc ổ đĩa (C:\ D:\, Thư mục gì đó) - Thực hiện chia sẻ qua mạng đối với thư mục dùng để Lưu trữ dữ liệu Backup (Everyone: Full control)
- Trên máy muốn backup thấy được Nơi lưu trữ dữ liệu backup đã chia sẻ - Trên máy Server cài đặt và cấu hình Backup /Recovery

#### d. Triển khai hệ thống ( Các bước thực hiện )

- Trên máy Server cài đặt và cấu hình Backup /Recovery
  - o Cài đặt Feature Windows Server Backup
    - o Tool → Windows Server Backup →Local Backup
    - o Thẻ Action →Backup One nếu muốn thực hiện một lần sao lưu ngay lập tức
      - Trong mục **Backup Options**, chọn **Different options** và nhấp vào **Next**.
      - Trong mục **Select Backup Configuration**, chọn **Full server (recommended)** để sao lưu tất cả dữ liệu máy chủ, ứng dụng và trạng thái hệ thống. Nhấp vào **Next**.
      - Trong mục **Specify Destination Type**, chọn **Remote shared folder** (Chọn nơi lưu trữ là địa chỉ mạng của nơi lưu dữ liệu backup) và nhấp vào **Next**.
      - Cung cấp thông tin đăng nhập của người dùng có quyền ghi vào thư mục mạng được chia sẻ.
      - Trong mục **Confirmation**, nhấp vào **Backup**.
  - o Thẻ Action → Backup Schedule nếu muốn lên lịch tự động sao lưu theo thời gian định sẵn
    - Mở **Windows Server Backup** và chọn **Local Backup** ở bên trái, sau đó nhấp vào **Backup Schedule** ở bên phải để cấu hình các quy tắc sao lưu tự động.
    - Trong mục **Getting Started**, nhấp vào **Next** để bắt đầu.
    - Trong mục **Select Backup Configuration**, chọn **Full server** nếu bạn muốn sao lưu toàn bộ hệ thống. Nếu không, chọn **Custom** để chỉ định một số tập tin hoặc thư mục cụ thể để sao lưu. Sau đó nhấp vào **Next**.
    - Trong mục **Specify Backup Time**, chọn thời gian để sao lưu hàng ngày hoặc nhiều lần trong ngày. Sau đó nhấp vào **Next**.
  - o Thẻ Action →Recovery để thực hiện khôi phục dữ liệu từ Backup Data Storage
    - Chọn vị trí lưu trữ bản sao lưu: **This server** hoặc **A backup stored in another location**. Nhấp vào **Next**.
    - Chỉ định đĩa cục bộ hoặc thư mục mạng nơi lưu trữ bản sao lưu và nhấp vào **Next**.

## **- File server.**

### **Ví dụ về File server:**

#### **Câu hỏi:**

Công ty ABC muốn xây dựng một hệ thống mạng nhằm mục đích chia sẻ dữ liệu nội bộ. Công ty có bốn phòng ban là Kế toán, kinh doanh, giám đốc và quản trị, nhân sự ở các phòng ban như sau: Phòng Kế toán gồm: Nguyễn Văn Tài, Trần Thị Minh. Phòng kinh doanh gồm: Lê An Tân, Nguyễn trúc Dương, Nguyễn Tuấn Đức. Phòng giám đốc gồm: Nguyễn Văn Tín, Đặng Văn Hiệu. Phòng quản trị gồm: Đặng Công Phụng, Nguyễn phúc Hưng. Và 50 nhân viên bán hàng. Ban giám đốc công ty muốn thực hiện tin học hóa với các yêu cầu thực hiện chia sẻ các thư mục như sau:

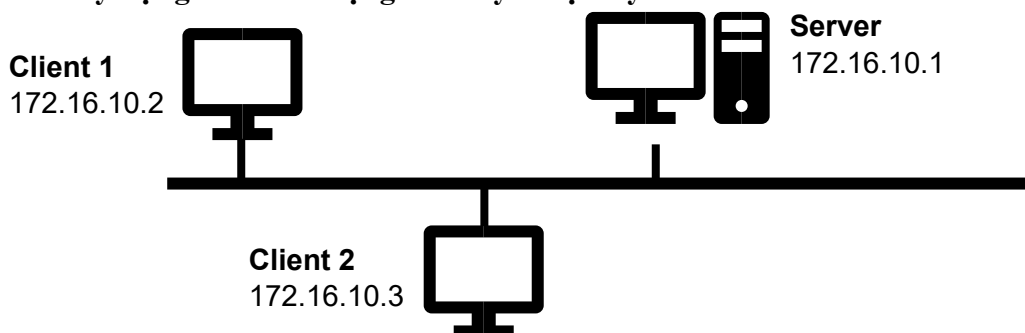
- Chia sẻ thư mục cha là thư mục Công ty cho toàn người dùng trên mạng có thể thấy và truy cập.
- Thư mục của phòng ban nào thì chỉ những người dùng của phòng ban đó mới có quyền truy cập vào.
- Trong từng phòng ban là từng thư mục cá nhân dành cho từng nhân viên trong phòng ban đó. Tương ứng với 1 thư mục người dùng thì chỉ có người đó mới có thể truy cập vào và có toàn quyền trên thư mục của mình. Ngoài ra trưởng phòng của bộ phận mà nhân viên đó đang trực thuộc cũng như Ban giám đốc cũng được quyền truy cập vào nhưng chỉ có quyền đọc mà thôi.
- Ban quản trị của công ty thì được toàn quyền trên tất cả các thư mục của phòng ban cũng như các thư mục của nhân viên trong công ty.
- Ban giám đốc được quyền truy xuất tới tất cả các thư mục của các phòng ban nhưng chỉ được quyền đọc. Ban giám đốc không được truy xuất tới các thư mục của Ban quản trị.

#### **Yêu cầu:**

- a. Xây dựng mô hình mạng và chuẩn bị máy ảo.
- b. Vận dụng kiến thức về File server, quyền NTFS Permission.
- c. Xác định các giải pháp thực hiện.
- d. Triển khai hệ thống mạng phù hợp với yêu cầu mô tả của công ty.

## Câu trả lời File server:

### a. Xây dựng mô hình mạng và chuyển bị máy ảo:



### b. Vận dụng kiến thức về File Server, quyền NTFS Permission:

File server tạm dịch là máy chủ tệp tin, là một hệ thống quản lý dữ liệu tập trung dựa vào mạng máy tính LAN, cho phép doanh nghiệp lưu trữ và quản lý dữ liệu tập chung trên server. Từ đó doanh nghiệp sẽ quản lý việc truy cập, quyền truy cập và sử dụng dữ liệu cùng từng nhân viên trong từng phòng ban hoặc từng nhóm làm việc. File server cung cấp địa điểm lưu trữ các tập tin máy tính được chia sẻ mà có thể được truy cập bởi các máy trạm làm việc trong mạng máy tính. Các tập tin ở đây là file âm thanh, hình ảnh, video, CSDL,... Cho phép người dùng chia sẻ qua mạng mà không cần phải sử dụng đĩa ngoài hoặc thiết bị lưu trữ khác.

NTFS Permission là hệ thống tập hợp các quyền cho phép hoặc không cho phép nhóm người dùng (Group) hay người dùng (User) truy cập vào các đối tượng chứa trên một phân vùng NTFS bao gồm thư mục và tập tin.

Các quyền cơ bản NTFS bao gồm:

- Full control (Toàn quyền): Cho phép người dùng có toàn quyền truy cập, chỉnh sửa và xóa thư mục hoặc tập tin
- Read : Cho phép người dùng đọc nội dung file
- List folder content: liệt kê nội dung folder ( User có thể mở folder để xem các file Subfolder)
- Read and excute: Có thể đọc nội dung các file và thực thi các file
- Write : Chỉnh sửa, tạo mới dữ liệu, ghi dữ liệu
- Modify: Có quyền Read, List Folder, Read and Execute; Write và Delete.

### c. Xác định các giải pháp thực hiện gồm:

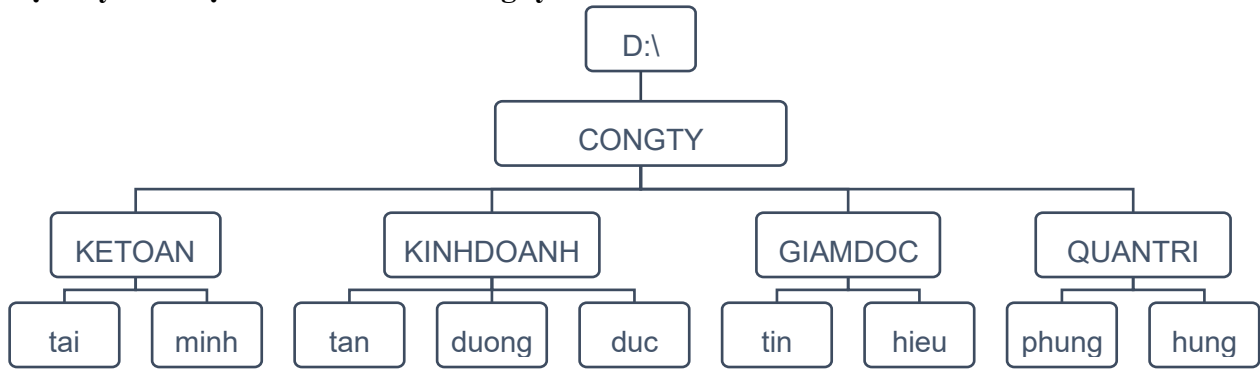
#### Tạo các user và Group theo mô tả như trên.

Trên máy Server tạo các tài khoản người dùng và tài khoản nhóm như sau:

- Nhóm **KETOAN** gồm: nvtai, ttminh
- Nhóm **KINHDOANH** gồm: lvtan, ntduong, ntduc
- Nhóm **GIAMDOC** gồm: nvtin, dvhieu
- Nhóm **QUANTRI** gồm: dcphung, nphung

*Ghi chú:* Một nhân viên có tên là Nguyễn Văn Tài sẽ có username: nvtai, password: nvtai và cú pháp GROUP;USER ( tên không dấu, không khoảng trắng, không ký tự đặc biệt, không vừa chữ thường vừa chữ hoa) hoặc gán tên các nhân viên thành kt1; kt2; qt1....(này hơi lâu)

Tạo cây thư mục theo mô tả của công ty:



Bản mô tả phân quyền NTFS trên các thư mục con cho phù hợp với yêu cầu:

	CONGTY
Everyone	<b>R</b>
QUANTRI	<b>F</b>

	KINHDOANH	tan	duong	duc
GIAMDOC	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>
QUANTRI	<b>F</b>	<b>F</b>	<b>F</b>	<b>F</b>
KINHDOANH	<b>R</b>			
latan	<b>R</b>	<b>F</b>	<b>R</b>	<b>R</b>
ntduong			<b>F</b>	
ntduc				<b>F</b>

	KETOAN	tai	minh
GIAMDOC	<b>R</b>	<b>R</b>	<b>R</b>
QUANTRI	<b>F</b>	<b>F</b>	<b>F</b>
KETOAN	<b>R</b>		
nvtai	<b>R</b>	<b>F</b>	<b>R</b>
ttminh			<b>F</b>

	GIAMDOC	tin	hieu
GIAMDOC	<b>R</b>		
QUANTRI	<b>F</b>	<b>F</b>	<b>F</b>
nvtin		<b>F</b>	<b>R</b>
dvhieu			<b>F</b>

	QUANTRI	phong	hung
QUANTRI	<b>R</b>		
dcphong		<b>F</b>	<b>R</b>
nphong			<b>F</b>



**Ghi chú:**

- F là Full control
- R là 3 quyền chính để truy xuất và thực thi được trên thư mục: Read & Execute, List Folder Content, Read

**d. Triển khai hệ thống mạng phù hợp với yêu cầu mô tả của công ty.****- Triển khai theo mô tả ở trên và thực hiện phân quyền**

Thực hiện phân quyền cho thư mục congtý sẽ kiểm tra đúng theo bảng mô tả

Thực hiện phân quyền cho thư mục kinhdoanh, tan, duong, duc

Thực hiện phân quyền cho thư mục ketoan, tai, minh

Thực hiện phân quyền cho thư mục Giamdoc, tin, hieu

Thực hiện phân quyền cho thư mục Quantri, phung, hung

*Thực hành và kiểm tra trên máy giáo viên Test kết quả.*

**- Chia sẻ các thư mục**

Thực hiện chia sẻ cho thư mục congtý sẽ kiểm tra đúng theo bảng mô tả

Thực hiện chia sẻ cho thư mục kinhdoanh, tan, duong, duc

Thực hiện chia sẻ cho thư mục ketoan, tai, minh

Thực hiện chia sẻ cho thư mục Giamdoc, tin, hieu

Thực hiện chia sẻ cho thư mục Quantri, phung, hung

*Thực hành và kiểm tra trên máy giáo viên Test kết quả.*

**CÂU 2:** Vận dụng nguyên lý ảo hóa để xác định các giải pháp thiết lập các dịch vụ ảo hóa hệ thống.

**Hiện thực:**

Vận dụng nguyên lý ảo hóa để thiết lập dịch vụ ảo hóa (Hyper-V, Xen, VMWare, KVM, VirtualBox, ...) để tạo nhiều máy ảo tương tác được với nhau

**Câu hỏi:**

Công ty abc có 200 người làm việc trong 3 phòng ban gồm: Phòng kế toán, phòng nhân sự, phòng đào tạo, dưới đây là thống kê các trang thiết bị mạng đã được công ty trang bị gồm:

- 1 máy Server IBM x3200 M3 có cấu hình: Processor: Intel® Xeon® Lynnfield Quad- Core X3430 2.4 GHz 8MB LGA 1156 95W, System Memory: 32G DDR- 3 1333 MHz ECC Memory, Storage: HDD SAS/SATA 3.5" Hot Swap, Network Controller: Dual Gigabit Ethernet 10/100/1000, Power: 1x Power Supply 430 watt 4x3.5", SATA/ SAS Driver Bay ...
- 200 máy tính để bàn CPU Dual Core E5200, Ram 2GB... - 15 máy tính xách tay cấu hình: CPU Core i5, Ram: 2GB...
- 20 máy in, 2 máy photo, scan
- Cùng một số thiết bị Switch, Router...
- Công ty đã thực hiện kết nối mạng nội bộ (mạng LAN) nhưng hệ thống mạng LAN chưa chuyên nghiệp và các thiết bị không tập trung tại Phòng Server nên khó khăn cho việc quản lý và khắc phục sự cố.
- Kết nối internet hiện tại chỉ sử dụng cho các nhu cầu đơn giản như sử dụng email, quản trị thông tin trang web của công ty, tra cứu, tìm kiếm thông tin,....
- Nhu cầu kết nối Internet của người dùng trong công ty tương đối cao nhưng hệ thống mạng của công ty lại không có thiết bị bảo mật (Firewall) chuyên dụng, dẫn đến việc mất an toàn thông tin là rất cao, dữ liệu công ty dễ dàng bị đánh cắp.
- Máy chủ hiện tại của công ty được sử dụng trong việc lưu trữ và chia sẻ tài nguyên nội bộ. Điều này khiến cho lượng tài nguyên và hiệu năng sử dụng của máy chủ chưa được tận dụng tối đa trong khi nhu cầu sử dụng máy chủ để chuyên trách đảm nhiệm thêm các nhu cầu thực tiễn khác trong công ty đang rất cần thiết. Để tiết kiệm chi phí, tận dụng tối đa hiệu năng của các thiết bị trên hệ thống hiện có, ban lãnh đạo công ty muốn triển khai hệ thống này bằng giải pháp ảo hóa, với tư cách là người chịu trách nhiệm về giải pháp IT của công ty.

**Yêu cầu:**

1. Hãy chọn công nghệ ảo hóa nào cho phù hợp với công ty? Giải thích vì sao chọn?
2. Đưa ra giải pháp thiết lập hệ thống ảo hóa cho công ty mà bạn đã chọn. Vẽ sơ đồ hệ thống các máy ảo kết nối với nhau, cấu hình IP các máy ảo và Ping được với nhau.

## **Câu trả lời:**

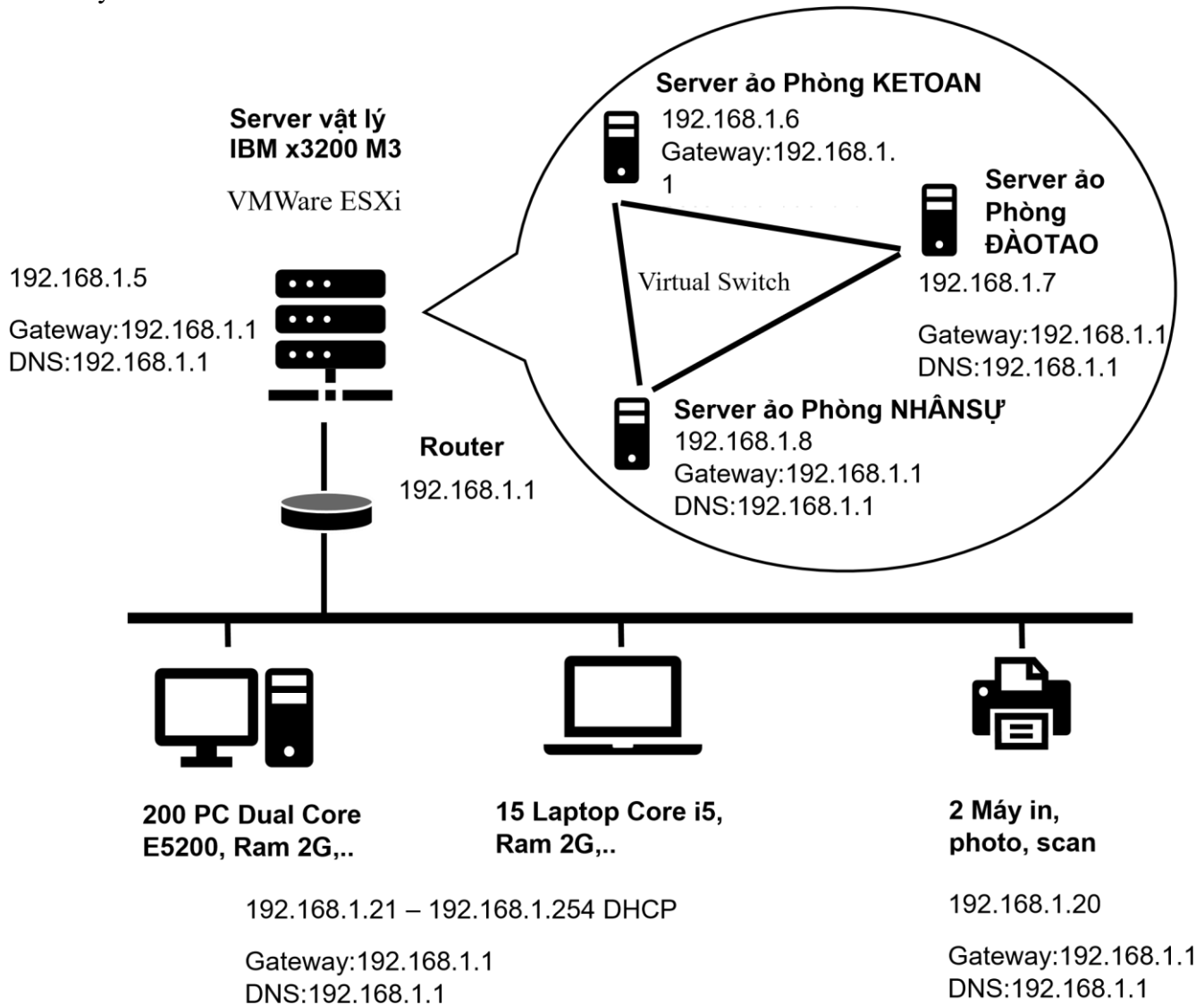
### **1. Công nghệ ảo hóa nào phù hợp với công ty?**

- Theo em, công nghệ ảo hóa phù hợp với công ty là ảo hóa máy chủ (server virtualization). Đây là công nghệ cho phép tạo ra nhiều máy chủ ảo (virtual server) trên một máy chủ vật lý (physical server), mỗi máy chủ ảo có thể chạy một hệ điều hành và các ứng dụng riêng biệt. Công nghệ này giúp tận dụng tối đa tài nguyên phần cứng của máy chủ vật lý, tiết kiệm chi phí đầu tư, bảo trì và điện năng, cũng như dễ dàng quản lý và mở rộng hệ thống. Đối với nhu cầu của công ty thì sẽ sử dụng ảo hóa VMWare ESXi, đây là công nghệ ảo hóa máy chủ loại 1. Miễn phí và đáng tin cậy, được sử dụng rộng rãi trên thị trường. VMWare ESXi có thể cài đặt trực tiếp lên máy chủ vật lý của công ty, không cần có hệ điều hành khác. VMWare ESXi có thể quản lý các máy ảo thông qua giao diện web hoặc phần mềm VMWare vSphere Client.

- Lý do chọn công nghệ này là vì công ty có nhu cầu sử dụng máy chủ cho ba phòng ban là **NHANSU; KETOAN; DAOTAO**. Nếu sử dụng ba máy chủ vật lý riêng biệt cho từng chức năng, sẽ gây lãng phí tài nguyên và chi phí, cũng như khó khăn trong việc bảo trì và nâng cấp. Nếu sử dụng một máy chủ vật lý duy nhất cho cả ba chức năng, sẽ gây ra xung đột cấu hình, thiếu nhất quán trong chính sách bảo mật và giảm hiệu suất của hệ thống. Do đó, việc sử dụng công nghệ ảo hóa máy chủ sẽ giải quyết được những vấn đề trên.

### **2. Giải pháp thiết lập hệ thống ảo hóa cho công ty:**

- Sau khi cài đặt VMWare ESXi, ta có thể tạo ra ba máy ảo trên máy chủ vật lý của công ty, mỗi máy ảo có cấu hình như sau:



#### Mô tả mô hình:

- Sử dụng máy Server IBM x3200 M3 làm máy chủ vật lý để chạy ảo hóa VMWare ESXi. Máy chủ này có địa chỉ IP là 192.168.1.5; Subnet mark:255.255.255.0; Default Gateway :192.168.1.1 ; DNS :192.168.1.1 . Được kết nối với LAN thông qua Switch.
- Tạo các máy ảo trên máy chủ vật lý. Ở đây ví dụ có 3 máy ảo **chạy các phòng ban**. Các máy ảo được chạy các hệ điều hành khác nhau để phù hợp với yêu cầu. Gán IP cho lần lượt các máy là 192.168.1.6 ; 192.168.1.7 ; 192.168.1.8 và Default Gateway và DNS cho cả 3 máy ảo là :192.168.1.1
- Các máy ảo được kết nối với nhau và với LAN công ty thông qua Virtual Switch của VMWare ESXi. Virtual Switch là một thiết bị mạng ảo được tạo ra trên VMWare ESXi, cho phép kết nối các máy ảo với nhau và với mạng LAN của công ty. Vswitch có thể được thiết lập các VLAN để biệt lập các nhóm máy ảo theo từng chức năng hoặc theo từng phòng ban
- 200 máy tính để bàn CPU Dual Core E5200, Ram 2GB,... và 15 máy tính xách tay CPU Core I5, Ram 2GB,... được cấp phát IP từ 192.168.1.33 đến 192.168.1.254; Subnet mark:255.255.255.0; Default Gateway và DNS : 192.168.1.1 bằng DHCP thông qua router

- 20 máy in, 2 máy photo,scan được đặt IP từ 192.168.1.10 đến 192.168.1.32 ; Subnet mark:255.255.255.0; Default Gateway và DNS : 192.168.1.1
- Các nhân viên có thể làm việc với máy ảo bằng cách Remote desktop (Điều khiển từ xa) thông qua địa chỉ IP máy ảo. Các thiết bị sẽ liên lạc với nhau thông qua địa chỉ IP của chúng
- Thiết lập các chính sách bảo mật cho máy ảo để đảm bảo an toàn thông tin của các tài liệu nội bộ, ví dụ như thiết lập quyền truy cập, mã hóa dữ liệu, sao lưu và khôi phục dữ liệu...