



I. Tóm tắt bài thực hành

1. Yêu cầu lý thuyết

Sinh viên đã được trang bị các kiến thức sau:

- Kiến trúc của hệ điều hành Windows Server.
- Các tính năng của hệ điều hành Windows Server.
- Dịch vụ thư mục Active Directory.
- Quản trị Active Directory.
- ...

2. Nội dung chính bài thực hành

- Triển khai cài đặt hệ điều hành Window Server 2016 (WS2016).
 - Tìm hiểu Computer Management, System Configuration.
 - Tìm hiểu các tiện ích cơ bản: Task manager, msconfig, sysedit.
 - Cấu hình Computer Name, IP và đánh giá kết quả.
 - Giới thiệu & sử dụng các lệnh ICMP: ping, ipconfig, pathping, tracert.
 - Tìm hiểu & sử dụng các câu lệnh net, net send, netsh, netstat.
 - Tiện ích Remote Desktop Connection.
- Triển khai dịch vụ Active Directory.
 - Tìm hiểu về Active Directory Domain Services.
 - Cài đặt Active Directory Domain Services và tên miền gốc.

II. Chi tiết bài thực hành

1. Cài cài đặt hệ điều hành Window Server 2016

a) Chuẩn bị

Chuẩn bị một máy vi tính có cấu hình cơ bản như sau:

- Processor architecture: x86-64
- Processor speed: 1.4 GHz
- Memory (RAM): 512 MB
- Hard disk space: 32 GB
- DVD ROM

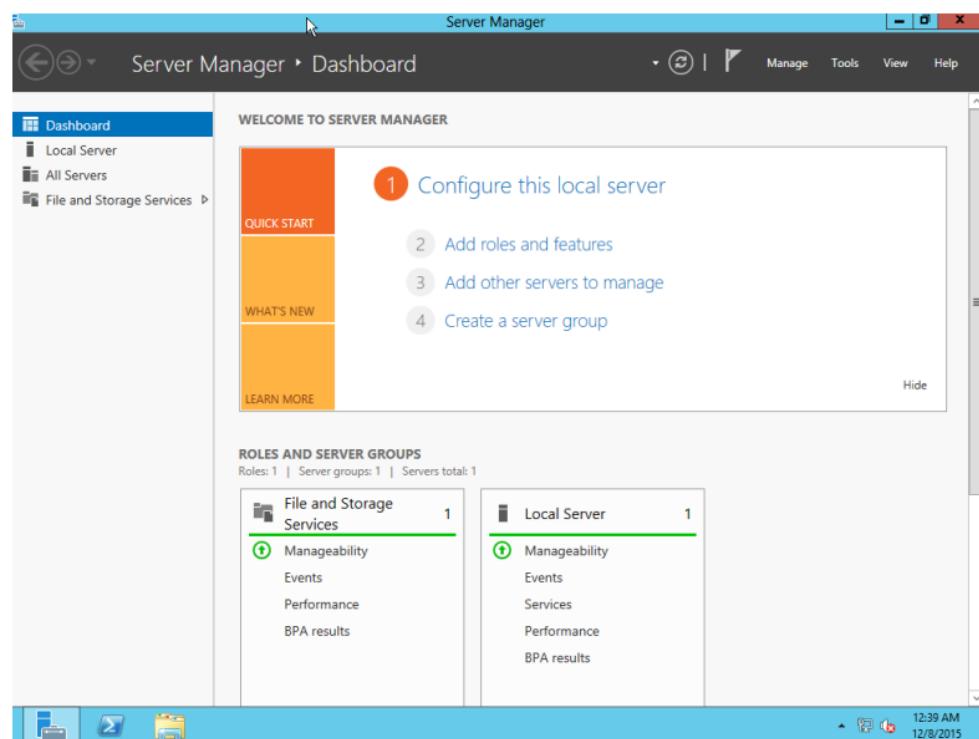
Cài đặt phần mềm VMware Workstation tạo các máy ảo.

b) Các bước cài đặt

Bước 1: Sinh viên tải về và cài đặt sẵn phần mềm [máy ảo VMWare Workstation](#)

Bước 2: Tải về file ISO của Hệ điều hành Window Server 2016

Bước 3: Sinh viên xem hướng dẫn cài đặt WS2016 trên máy ảo VMWare [tại đây](#) hoặc có thể tham khảo các nguồn hướng dẫn khác. Sau khi thực hiện cài đặt và các cấu hình liên quan khác, khởi động lại hệ điều hành WS2016 trên máy ảo, mặc định màn hình Server Manager hiện ra nhu hình 1. Lưu ý **đặt tên cho máy chạy WS2016 theo cú pháp sau: [WS2016_MSSV]**.

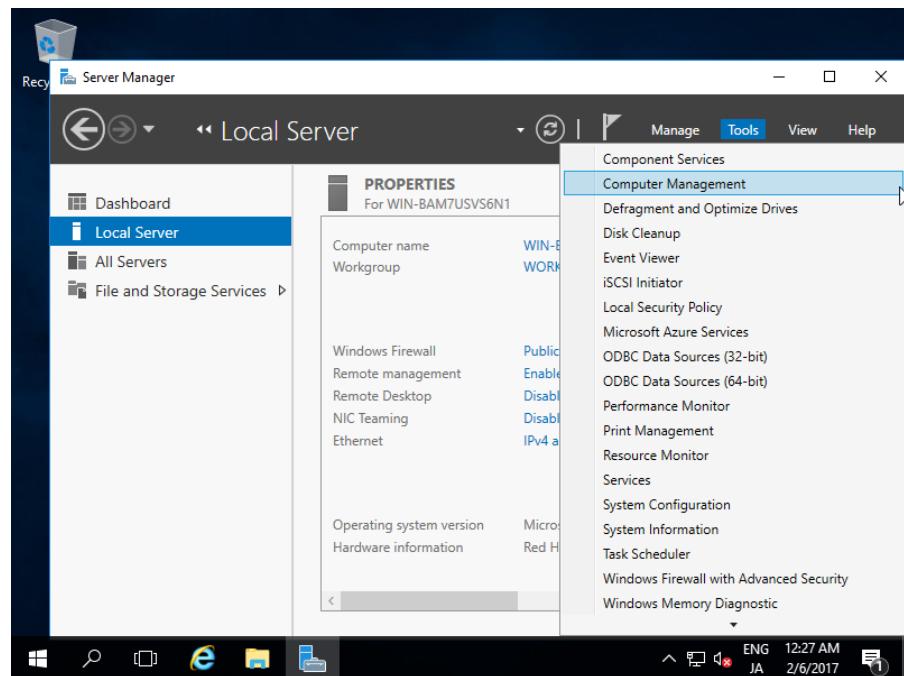


Hình 1: Màn hình Server Manager trên WS2016

2. Một số thao tác cơ bản với Computer Management và System Configuration trên WS 2016

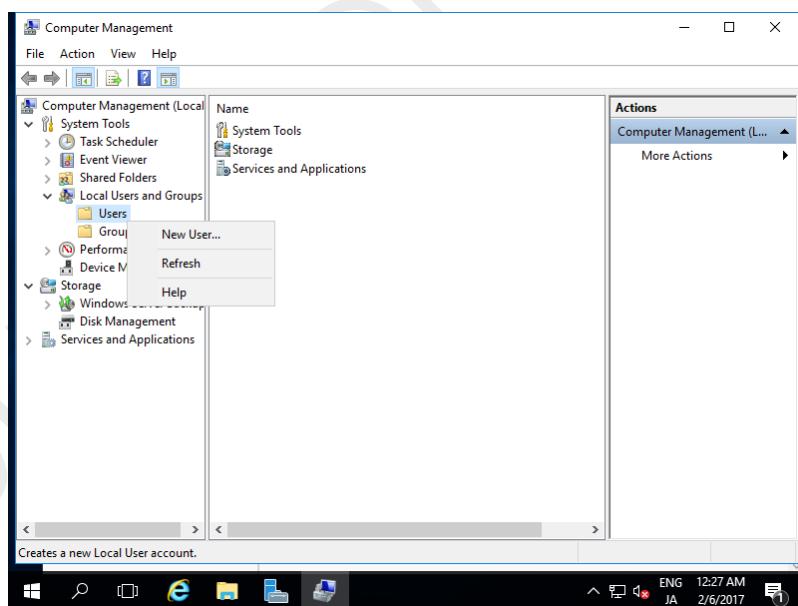
a) Thêm tài khoản người dùng cục bộ (Add local user)

Bước 1: Vào [Server Manager] → [Tools] → [Computer Management] như hình 2.



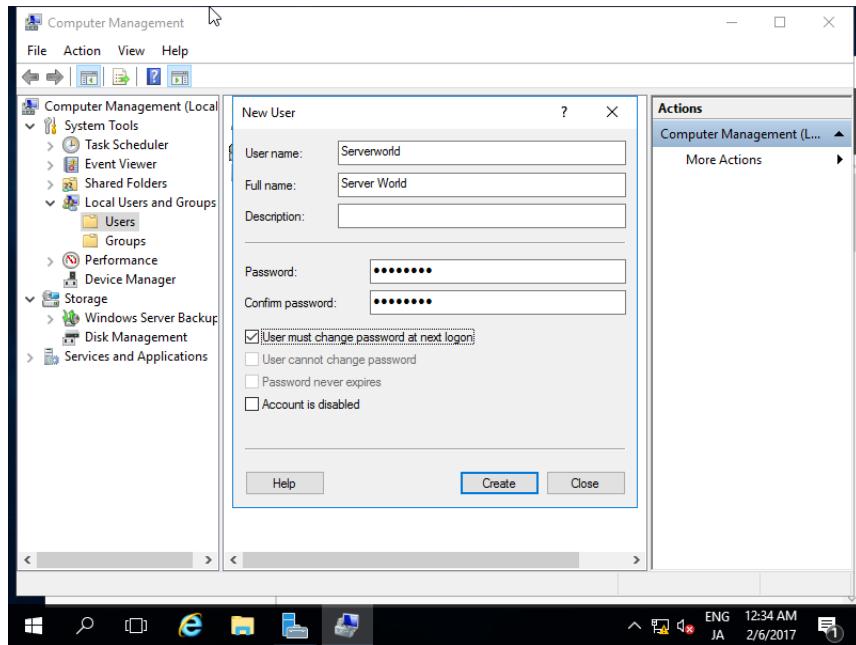
Hình 2: Minh họa bước 1

Bước 2: Click chuột phải vào [Users] ở dưới [Local Users and Groups] ở phần ô phía bên trái và lựa chọn [New User] như hình 3.



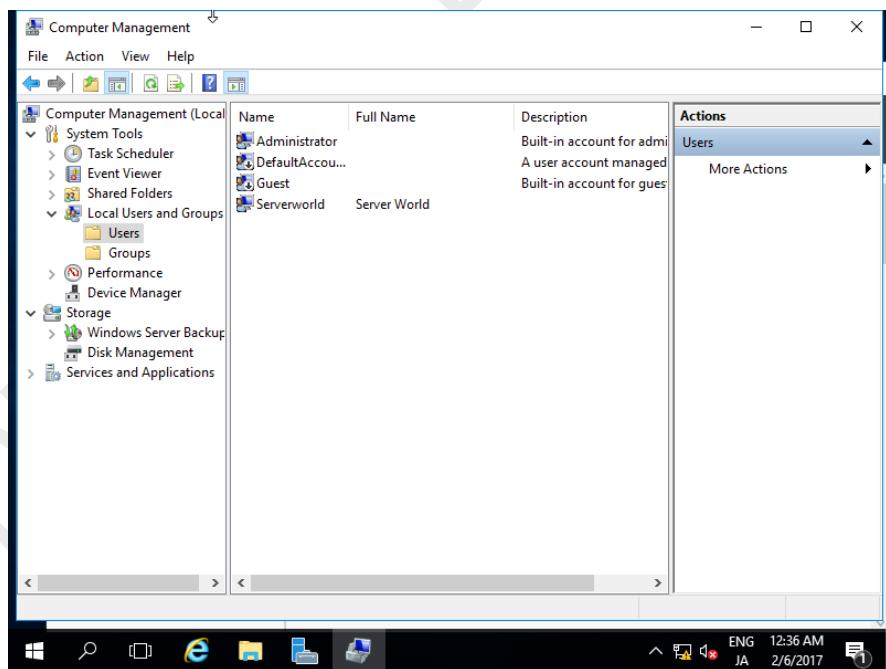
Hình 3: Minh họa bước 2

Bước 3: Nhập vào Username và Password cho người dùng mới và click nút [Create].
Những trường dữ liệu khác có thể để trống như hình 4.



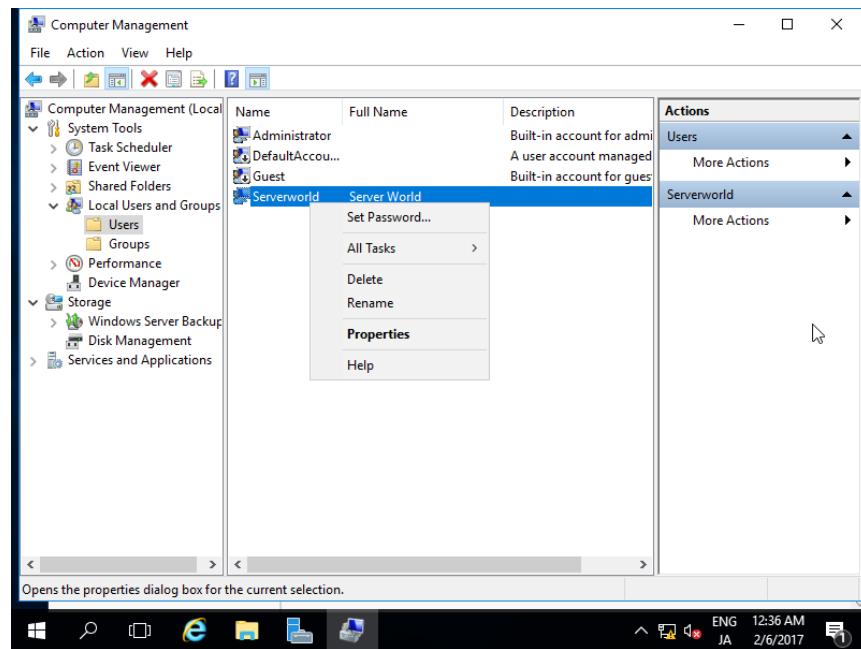
Hình 4: Minh họa bước 3

Bước 4: Sau khi tạo tài khoản thành công sẽ xuất hiện tài khoản vừa tạo trong danh sách như hình 5.



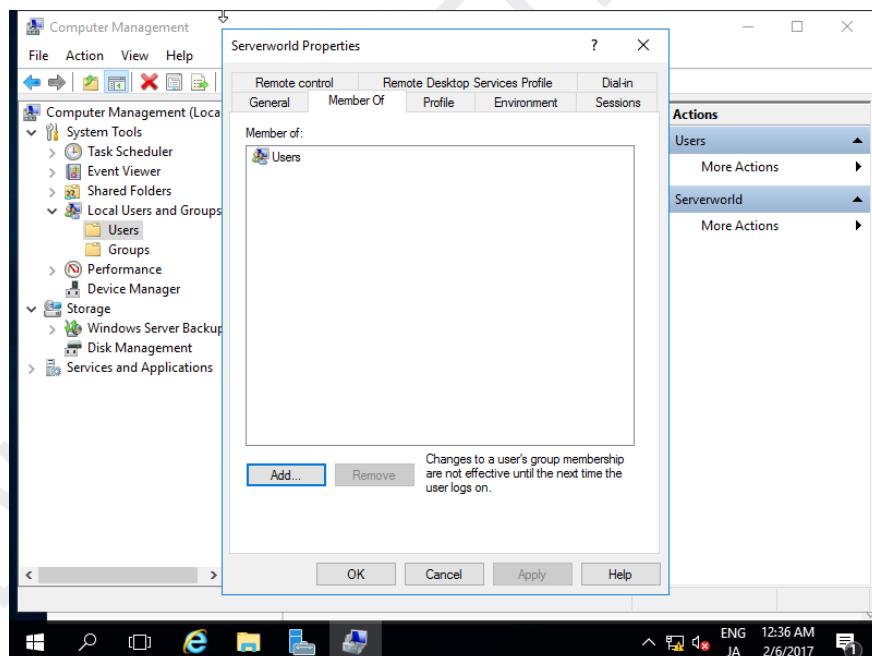
Hình 5: Minh họa bước 4

Bước 5: Nếu muốn đặt đặc quyền quản trị (administrative privilege) cho người dùng mới, hãy nhấp chuột phải vào người dùng đó và mở [Properties].



Hình 6: Minh họa bước 5

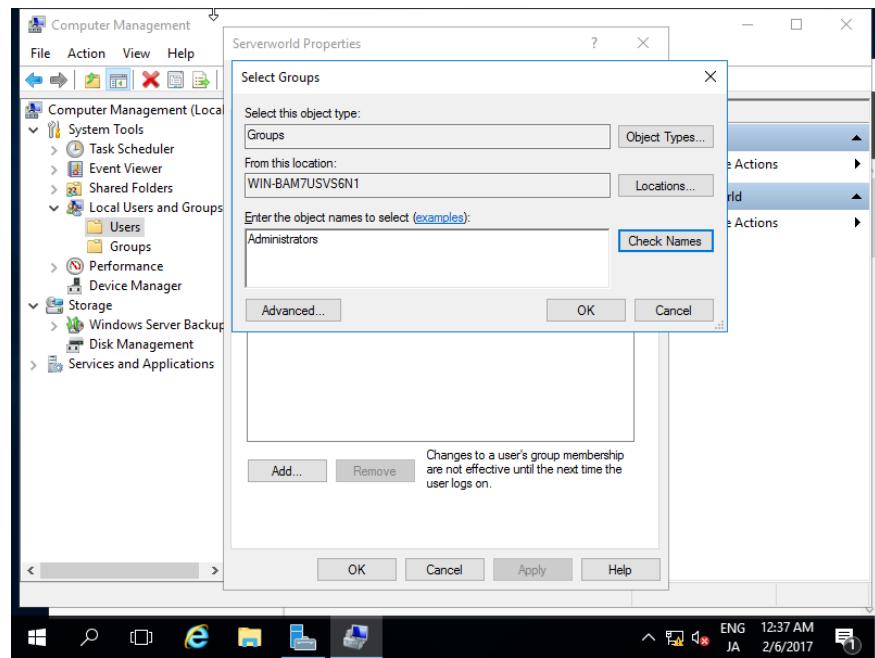
Bước 6: Di chuyển tới tab [Member] và nhấp nút [Add] như hình 7.



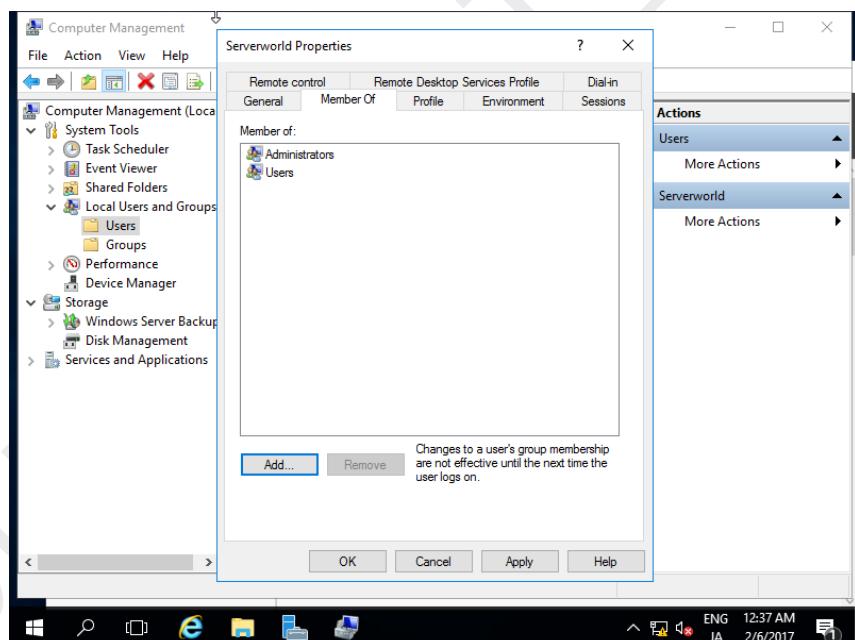
Hình 7: Minh họa bước 6

Bước 7: Chỉ định nhóm [Administrator] như hình 8.

Bước 8: Đảm bảo nhóm [Administrator] được thêm vào danh sách như hình 9 và nhấp vào nút [OK] để hoàn tất cài đặt.



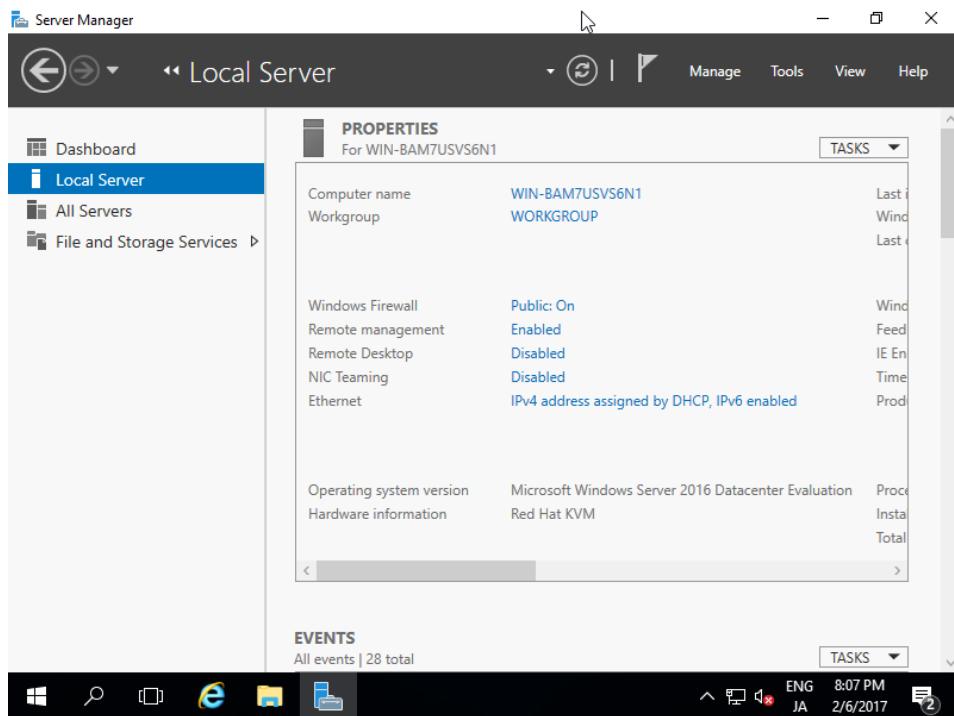
Hình 8: Minh họa bước 7



Hình 9: Minh họa bước 8

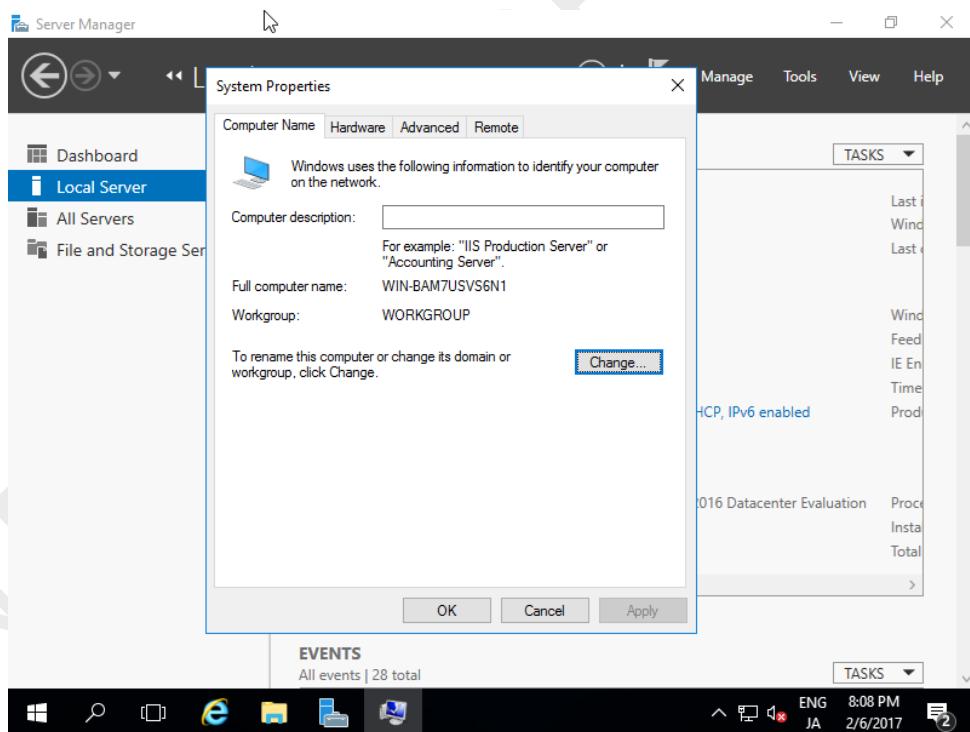
b) Cài đặt tên máy tính

Bước 1: Chạy [Server Manager] và chọn [Local Server] ở khung bên trái và nhấp vào phần [Computer Name] ở khung bên phải như hình 10.



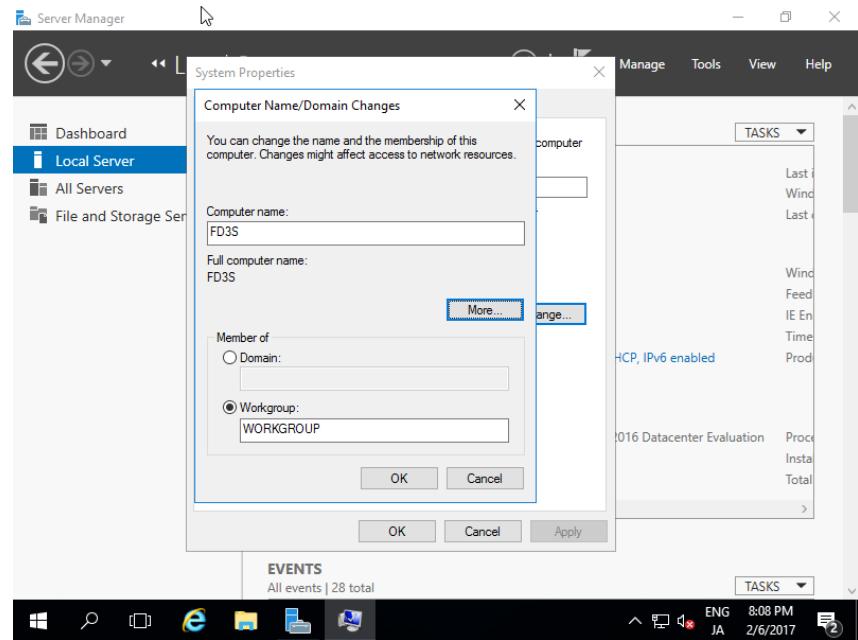
Hình 10: Minh họa bước 1

Bước 2: Di chuyển tới tab [ComputerName] và click nút [Change] như hình 11.



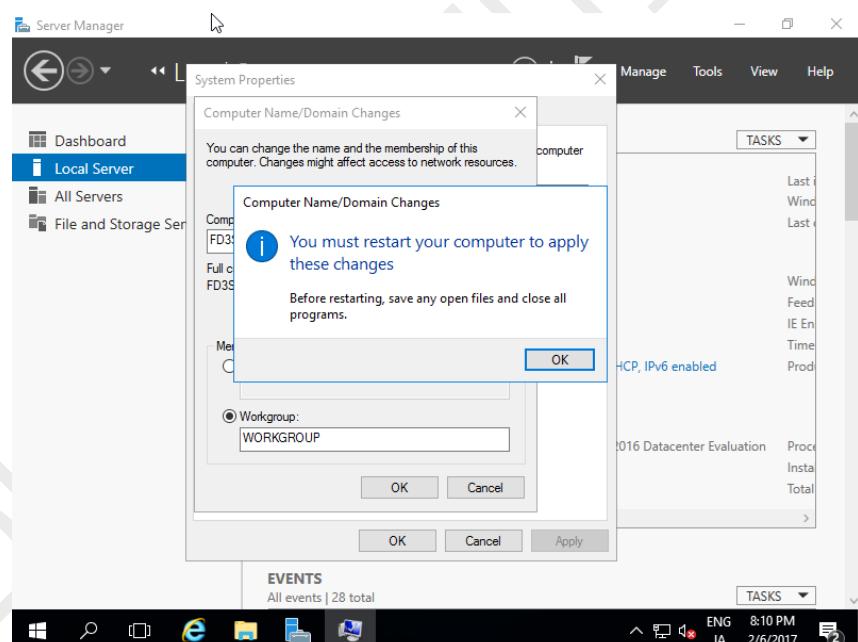
Hình 11: Minh họa bước 2

Bước 3: Nhập bất kỳ Tên máy tính nào vào trường [ComputerName] và tiếp theo, nhấp vào nút [More...] như hình 12.



Hình 12: Minh họa bước 3

Bước 4: Khởi động lại máy tính để hoàn tất việc cài đặt tên máy tính.



Hình 13: Minh họa bước 4

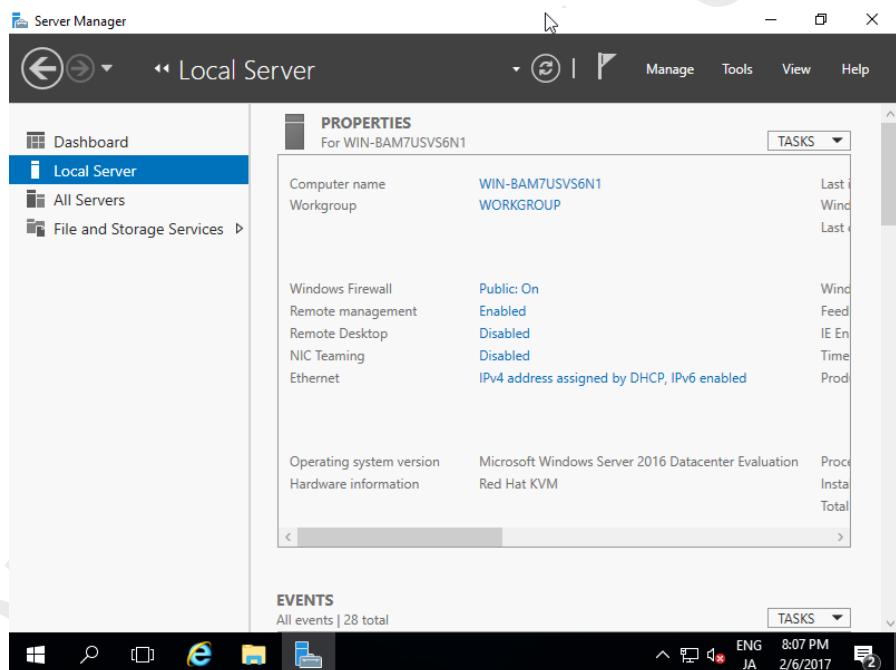
Bước 5: Ngoài ra, còn có thể đổi tên máy tính thông qua các câu lệnh trên màn hình Command Prompt như sau:

- Mở màn hình Command prompt, chạy theo quyền [Run as administrator].
- Nhập lệnh: >hostname
- Nhập lệnh: Netdom renamecomputer %ComputerName% /NewName: NewComputerName

c) Cài đặt địa chỉ IP tĩnh cho máy tính

Như đã biết, mặc định khi một thiết bị tham gia vào môi trường Internet sẽ được gán một địa chỉ IP riêng biệt để có thể giao tiếp với các thiết bị khác trong môi trường. Nhờ vào dịch vụ cấp phát địa chỉ IP (gọi là DHCP) tự động cấp phát một địa chỉ IP riêng biệt cho các thiết bị trong mạng mà không cần phải cấu hình thủ công. DHCP kiểm soát việc cấp phát địa chỉ IP để tránh xung đột địa chỉ IP trong mạng. Khi một thiết bị kết nối vào mạng, DHCP sẽ tự động kiểm tra và đảm bảo rằng địa chỉ IP cung cấp cho thiết bị đó chưa được sử dụng. Tuy nhiên, với hệ điều hành WS 2016, người quản trị mạng còn có thể tự cấu hình địa chỉ IP (địa chỉ IPv4) cho thiết bị trong môi trường mạng theo các bước sau:

Bước 1: Chạy [Server Manager] và chọn [Local Server] ở khung bên trái và nhấp vào phần [Ethernet] ở khung bên phải như hình 14.

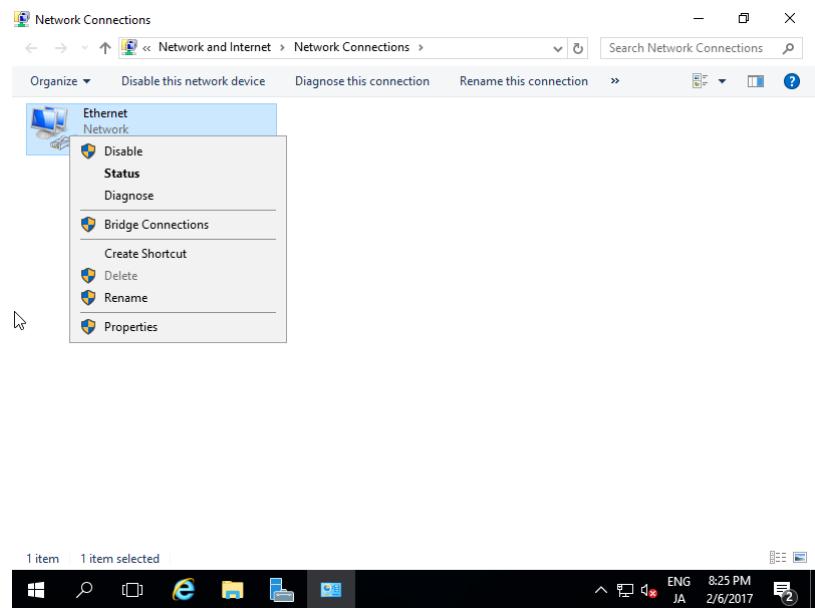


Hình 14: Minh họa bước 1

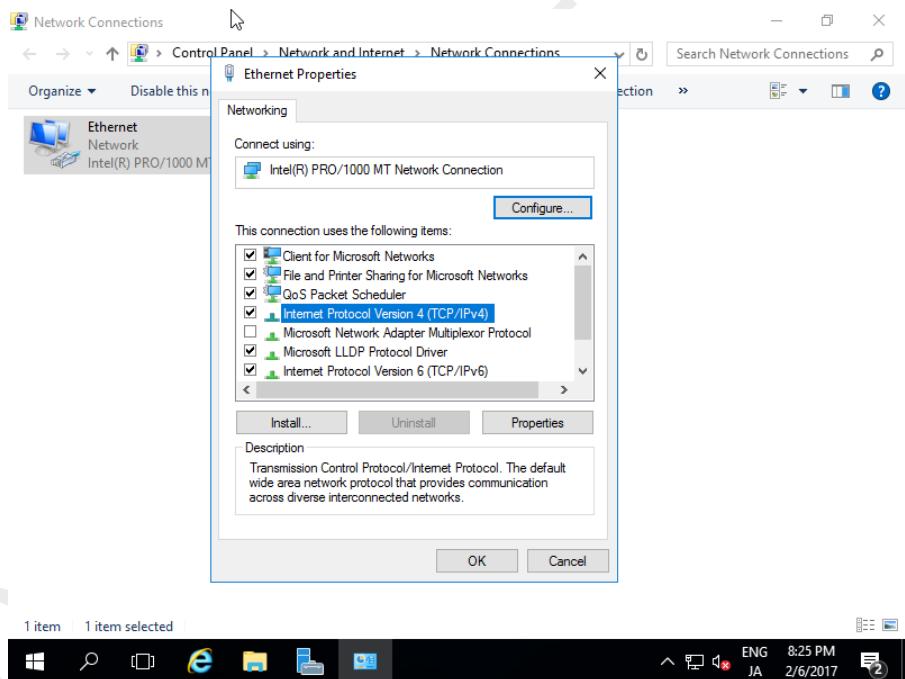
Bước 2: Nhấp chuột phải vào biểu tượng [Ethernet] và mở [Properties] như hình 15.

Bước 3: Chọn [Internet Protocol Version 4] và nhấp vào nút [Properties] như hình 16

Bước 4: Cài đặt lại các thông số sau dựa theo thông tin mạng LAN đang dùng như hình 17: IP address, Subnet Mask, preferred DNS Server, default Gateway.



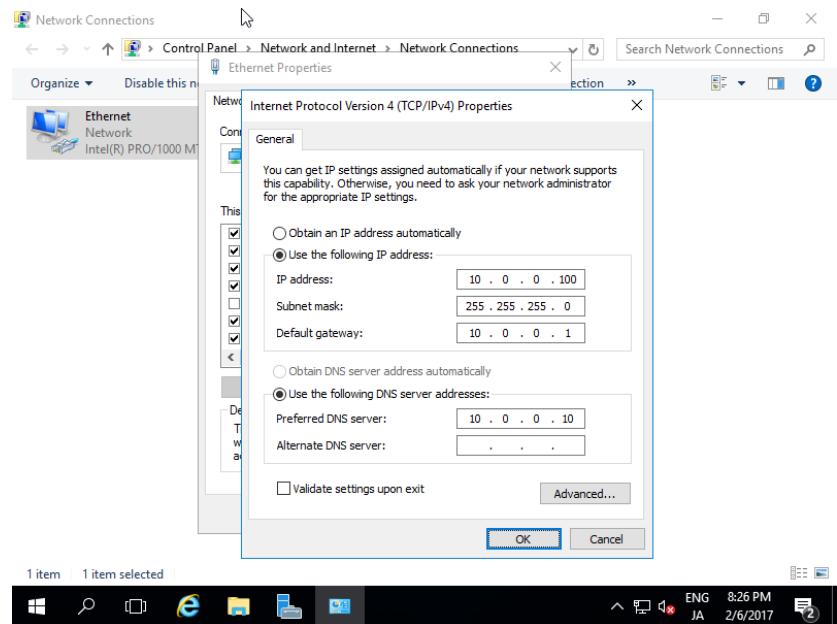
Hình 15: Minh họa bước 2



Hình 16: Minh họa bước 3

Bước 5: Bên cạnh đó, còn có thể cài đặt địa chỉ IPv4 cho máy tính thông qua các câu lệnh trên Command Prompt như sau:

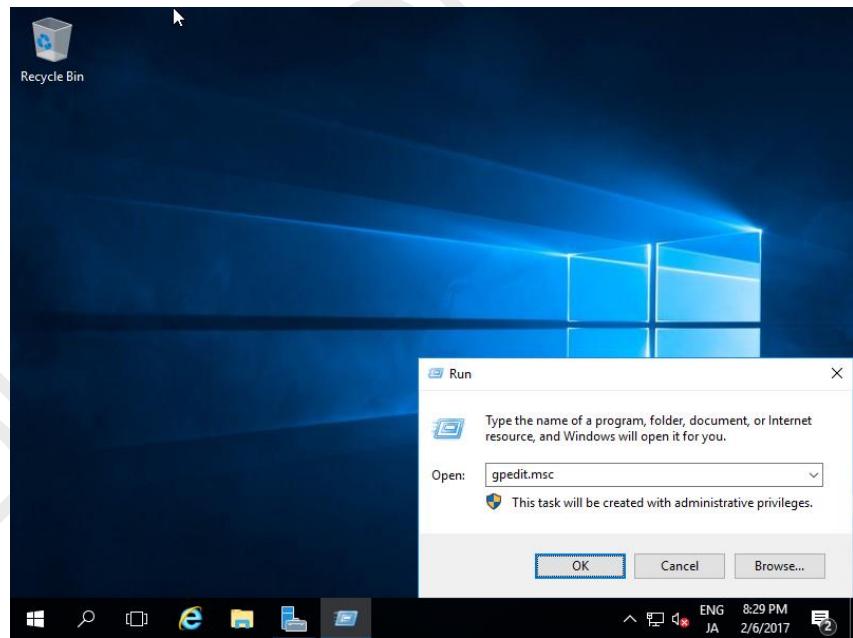
- Mở màn hình Command prompt, chạy theo quyền [Run as administrator].
- Nhập lệnh: cmd> netsh interface ipv4 show interfaces
- Nhập lệnh: cmd> Netsh interface ipv4 add dnsserver name=Ethernet address= [Địa chỉ IP] index=1
- Nhập lệnh: cmd> IPconfig /all



Hình 17: Minh họa bước 4

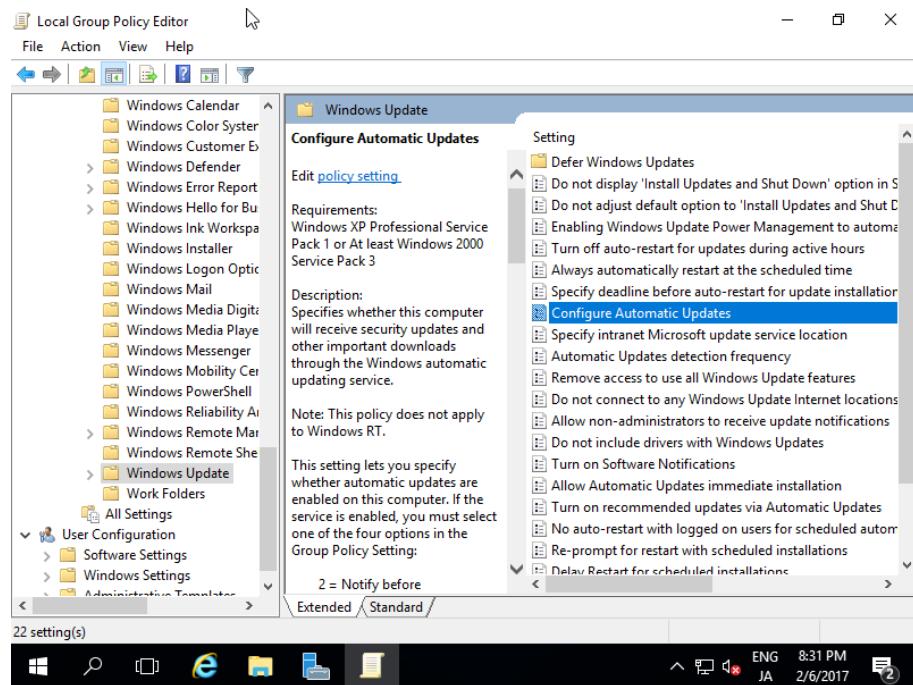
d) Kích hoạt chức năng tự động cập nhật hệ điều hành

Bước 1: Vào khung tìm kiếm, nhập lệnh [Run] sau đó nhập lệnh [gpedit.msc] như hình 18.



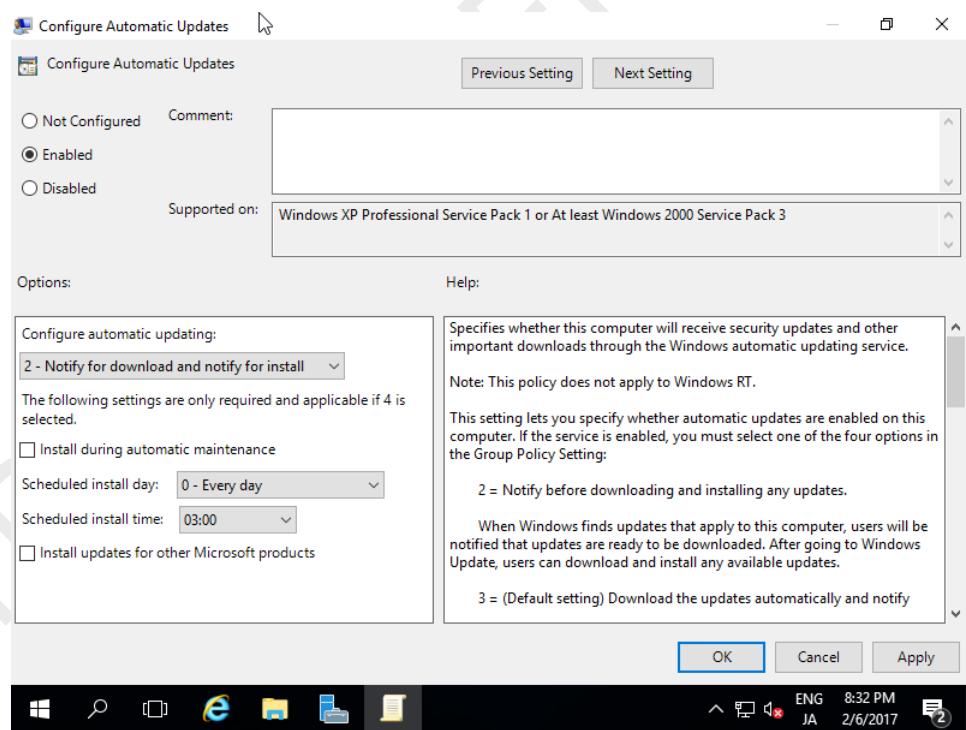
Hình 18: Minh họa bước 1

Bước 2: Chọn [Administrative Template] - [Cấu phần Windows] - [Windows Components] ở khung bên trái và nhập vào [Configure Automatic Updates] để mở ở khung bên phải.



Hình 19: Minh họa bước 2

Bước 3: Định cấu hình cài đặt Windows Update mà bạn muốn.



Hình 20: Minh họa bước 3

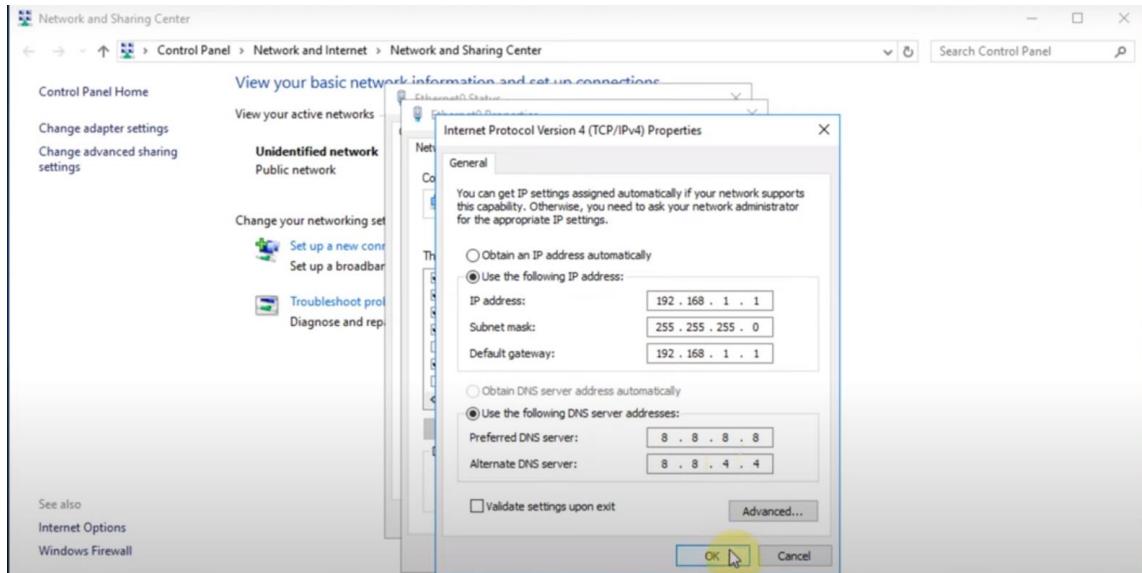
e) Chức năng Remote Desktop Connection

Trong phần này, sinh viên sẽ thực hiện demo chức năng chia sẻ tài nguyên giữa hai máy tính cài hai hệ điều hành khác nhau là WS2016 và Window 7/8/10 trên cùng một máy ảo. Trình tự các bước thực hiện như sau:

Bước 1: Trên máy ảo VMWare, sinh viên cài thêm máy client dùng hệ điều hành Window 7/8/10. Có thể tham khảo hướng dẫn tại [đây](#). Lưu ý đặt tên cho máy chạy Window 7/8/10 theo cú pháp sau: [Win7810_MSSV].

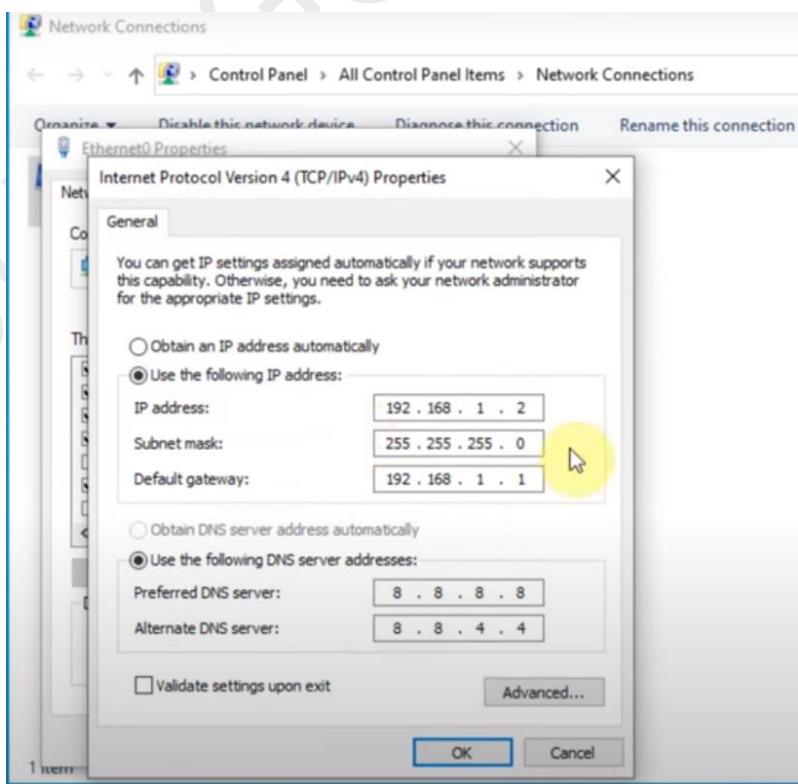
Bước 2: Cấu hình địa chỉ IP cho các máy tính như sau:

- Máy tính WS2016: 192.168.1.1 / 255.255.255.0 (hình 21)



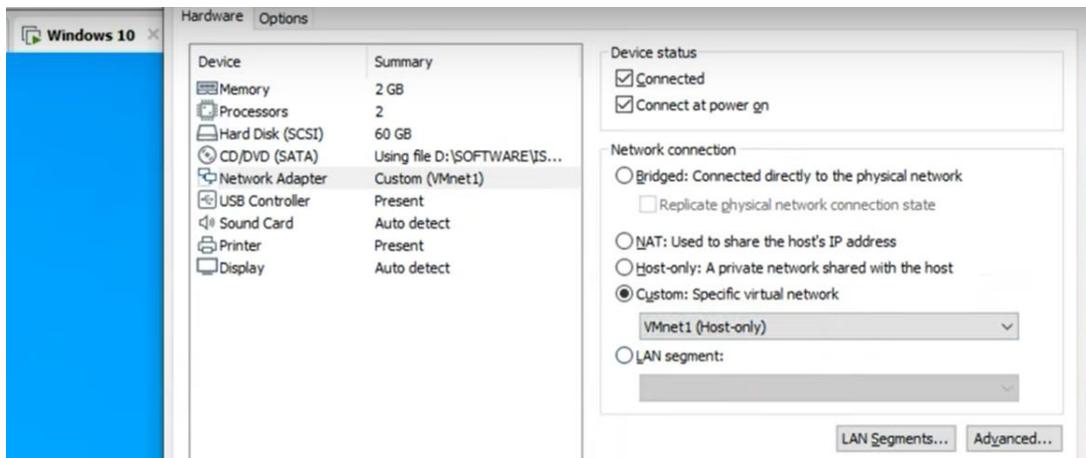
Hình 21: Cấu hình địa chỉ IP cho máy WS2016

- Máy tính Window 7/8/10: 192.168.1.2 / 255.255.255.0 (hình 22)

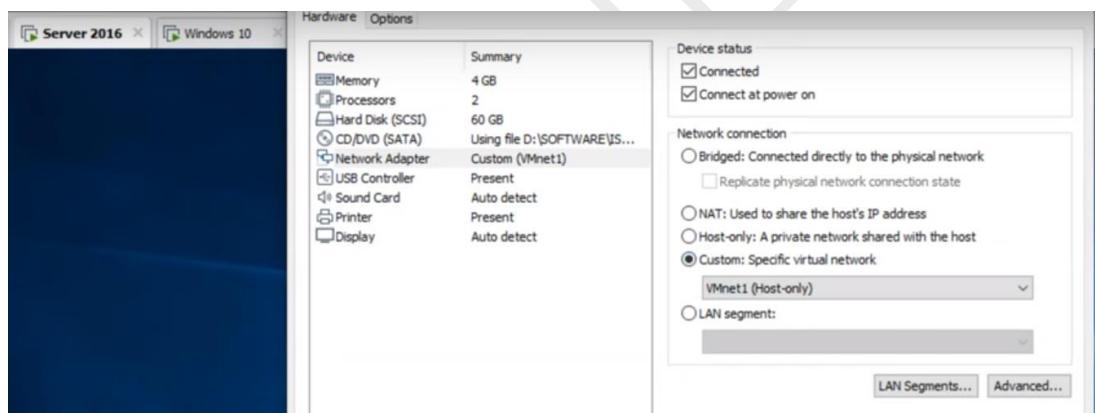


Hình 22: Cấu hình địa chỉ IP cho máy Window

Bước 3: Cài đặt card mạng cùng chế độ “VMNet1” cho cả 2 máy trên VMWare như hình 23 (máy Window 7/8/10) và hình 24 (máy WS2016). Trên thanh công cụ vào tab VM → Setting → Tab HardWare → Netword Adapter → Tùy chọn Custom: Specific virtual network → Chọn VMnet1 (Host - only).



Hình 23: Cài đặt card mạng trên máy Window 7/8/10



Hình 24: Cài đặt card mạng trên máy WS2016

Bước 4: Kiểm tra xem cả hai máy đã kết nối vào cùng một môi trường mạng hay chưa bằng cách thực hiện lệnh ping địa chỉ IP cho mỗi máy theo như hình 25 và hình 26. Trong trường hợp sau khi ping địa chỉ IP ở cả hai máy mà không xuất hiện kết quả như hình 25 và 26 thì cần kiểm tra xem firewall của mỗi máy đã được tạm thời tắt hay chưa.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1055]
(c) Microsoft Corporation. All rights reserved.

C:\Users\win10>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\win10>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=3ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\Users\win10>
```

Hình 25: Trạng thái kết nối vào môi trường mạng của máy Window 7/8/10

```
C:\Windows\system32\cmd.exe
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.1.2

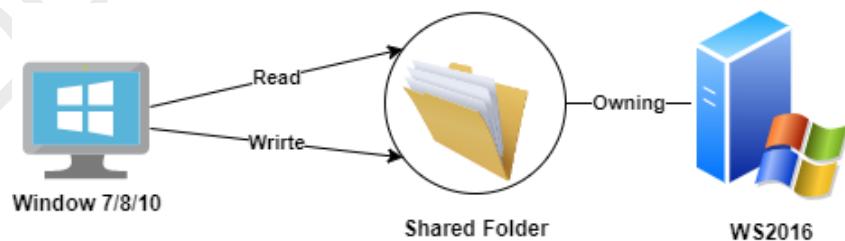
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>
```

Hình 26: Trạng thái kết nối vào môi trường mạng của máy W2016

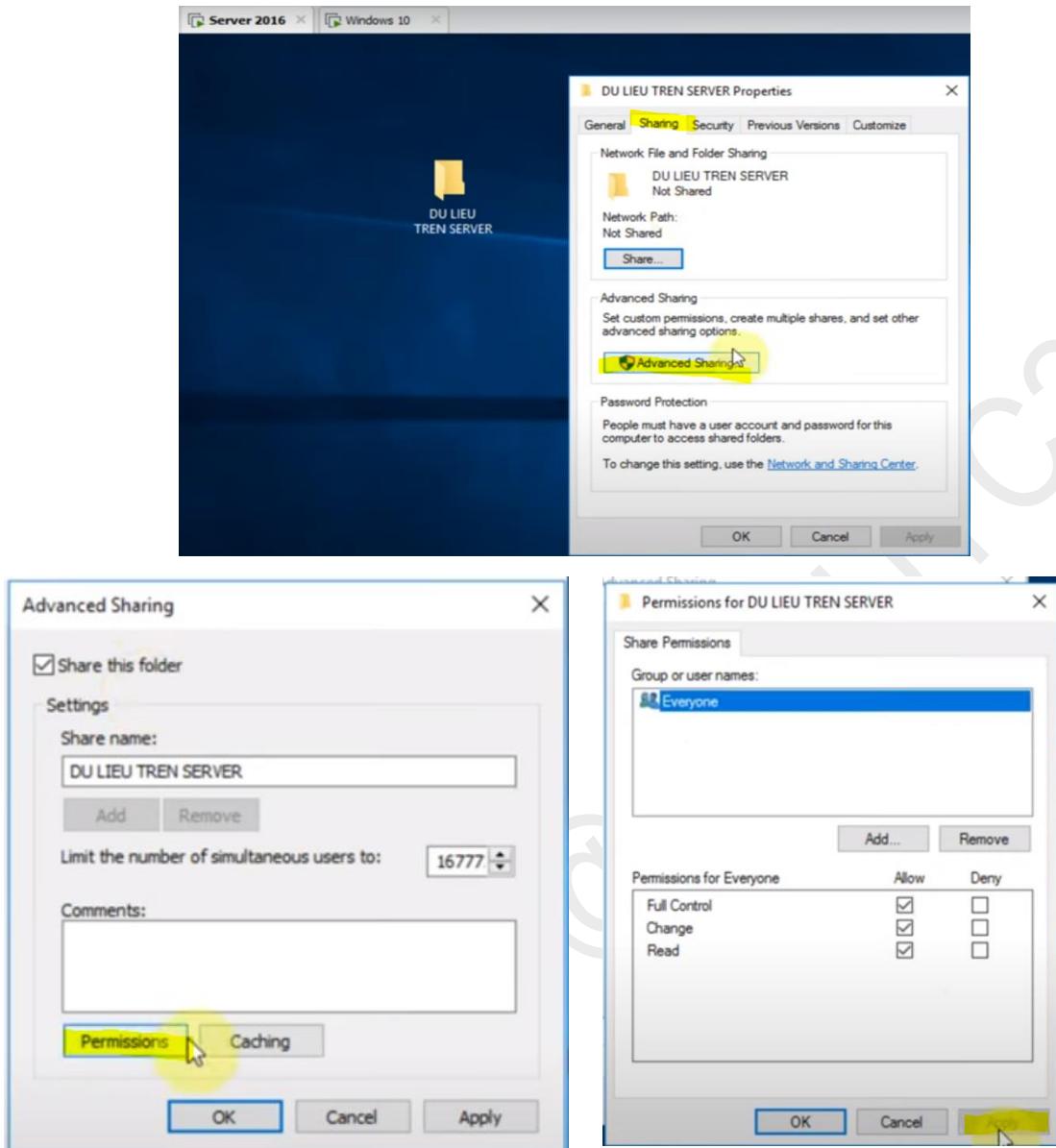
Bước 5: Sau khi đã chắc chắn cả hai máy đều đã tham gia vào cùng một môi trường mạng, tiếp theo sẽ kiểm tra kết nối giữa hai máy với một trường hợp có thể chia sẻ tài nguyên giữa hai máy này theo hình minh họa 27.



Hình 27: Minh họa việc chia sẻ tài nguyên giữa hai máy.

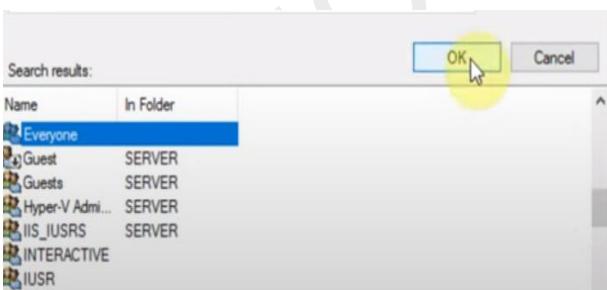
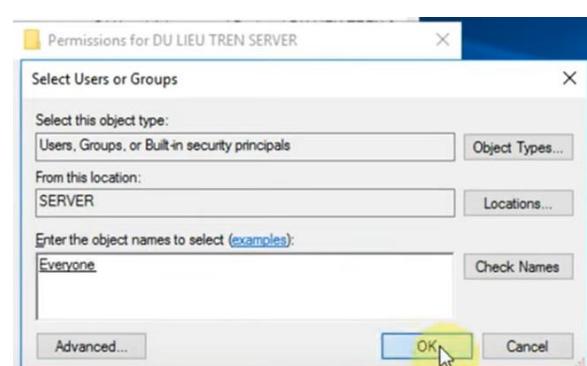
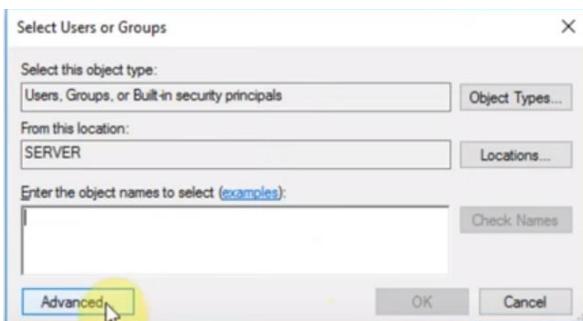
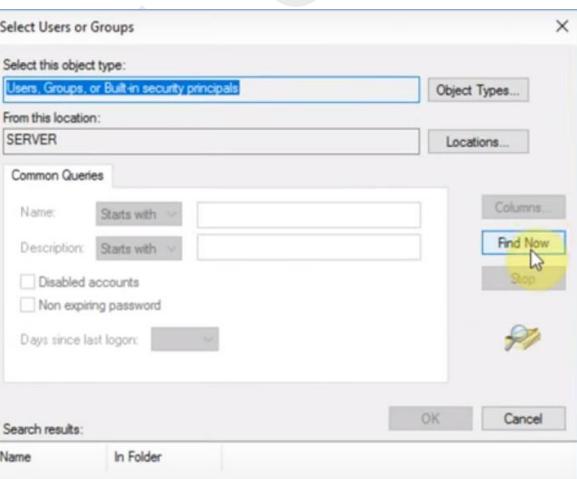
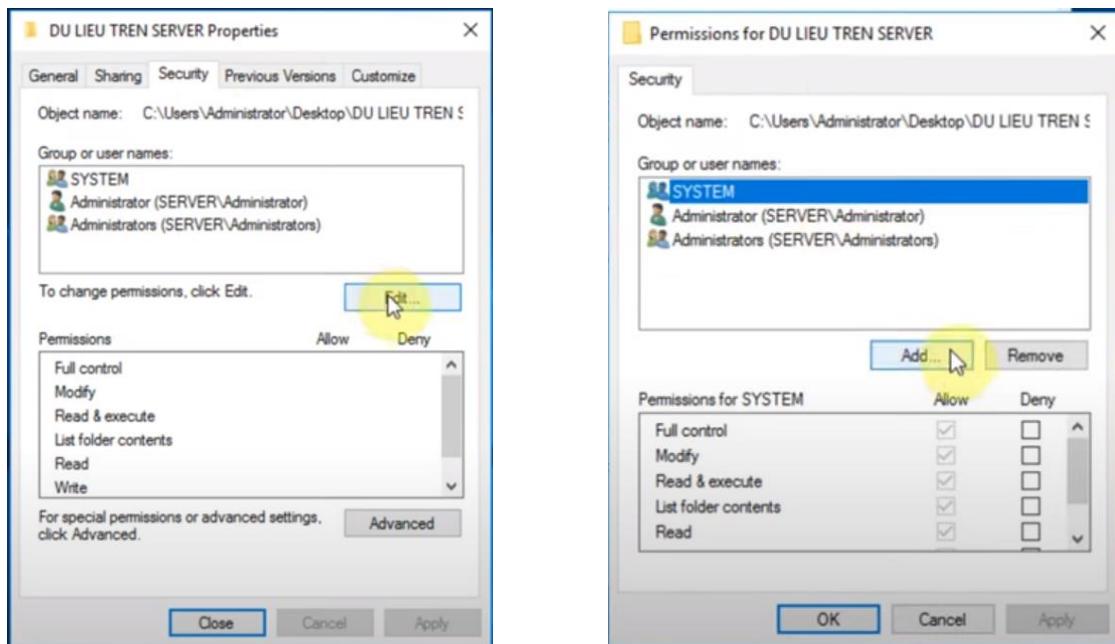
Cụ thể, các bước demo như sau:

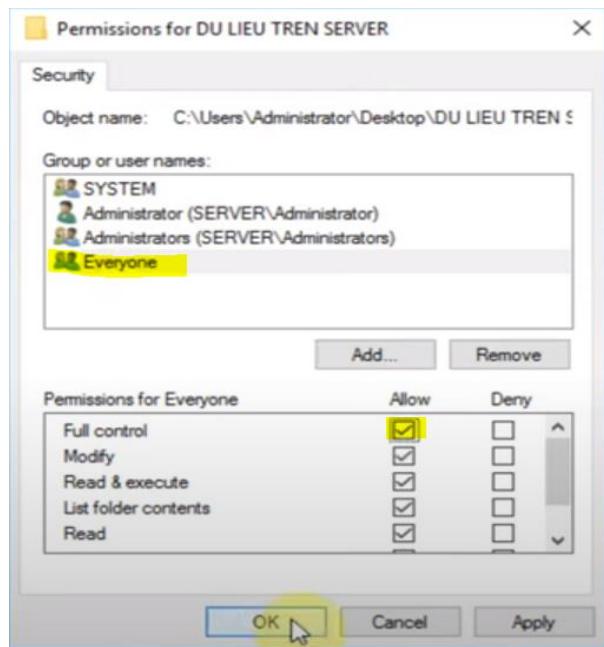
- Trên máy WS2016, tạo một thư mục đặt tên theo cú pháp **[Shared_MSSV]**.
- Click chuột phải vào thư mục, cài đặt Properties cho thư mục như sau:
 - Tab Sharing: chọn Group user là “Everyone” với Permission là “Full control”. Các bước thực hiện như các hình 28.



Hình 28: Minh họa các bước trên tab Sharing

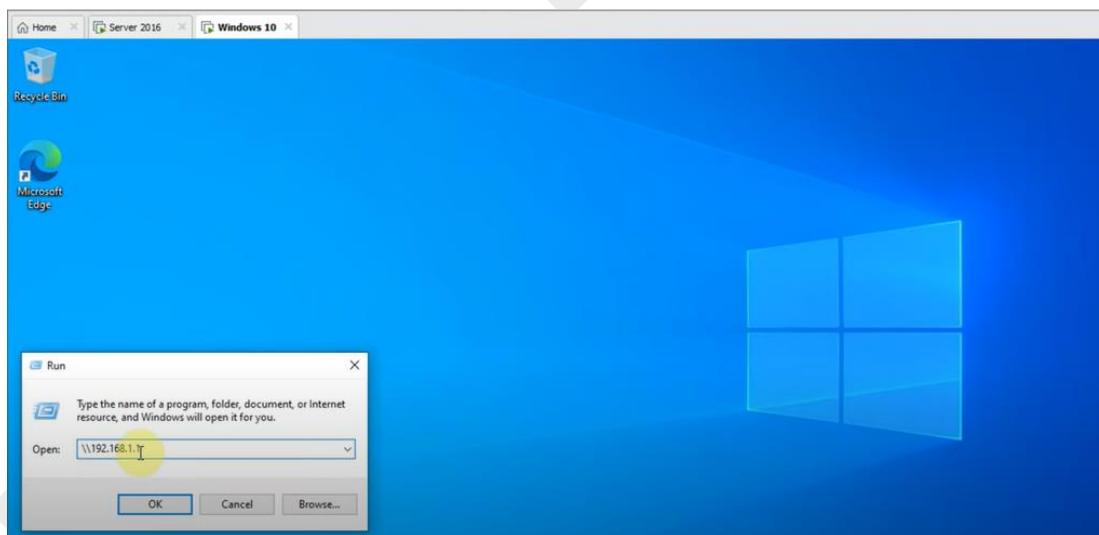
- Tab Security: chọn Group user là “Everyone” với Permission là “Full control”. Các bước thực hiện như các hình 29.





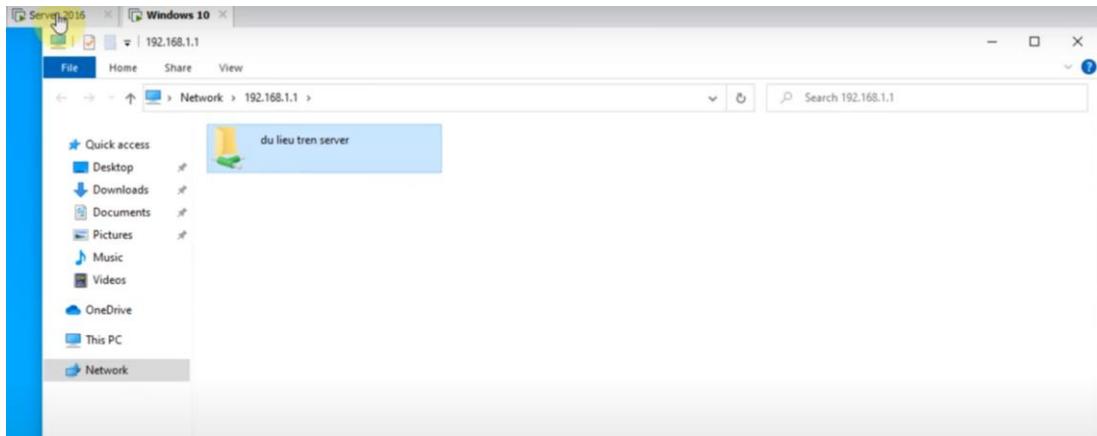
Hình 29: Minh họa các bước trong tab Security

- Kết nối vào thư mục [Shared_MSSV] từ máy tính Window 7/8/10. Gõ lệnh Run trên thanh tìm kiếm → nhập địa chỉ \192.168.1.1 như hình 30.



Hình 30: Kết nối vào máy tính WS2016 từ máy tính Window 7/8/10

- Xuất hiện hộp thoại yêu cầu nhập thông tin xác thực của user được kết nối đến máy WS2016. Mặc định ban đầu ta sẽ sử dụng thông tin tài khoản của user “Administrator” đã cài đặt trên máy WS2016. Sau khi nhập xong ta sẽ có thể truy cập vào thư mục vừa tạo từ máy Window 7/8/10 như hình 30.



Hình 31: Kết quả sau khi kết nối thành công.

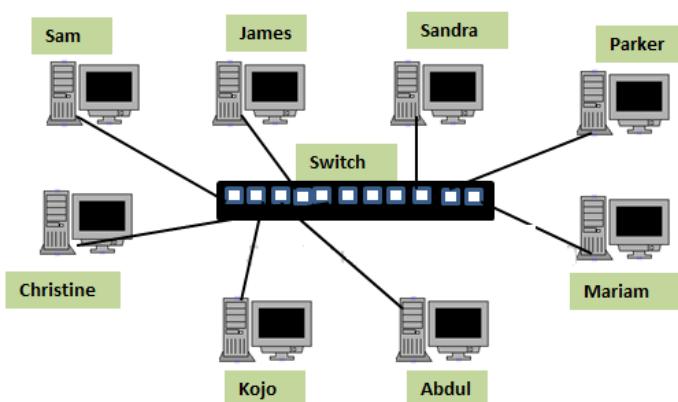
- Tuy nhiên trong thực tế nếu để người dùng bất kì được truy cập vào máy chủ WS2016 với toàn quyền quản trị thì sẽ rất nguy hiểm với vấn đề bảo mật. Do đó, cần phải tạo tài khoản xác thực tương ứng cho người dùng được phép truy cập vào. Cụ thể, sinh viên thực hiện tạo một tài khoản xác thực trên WS2016 (tham khảo mục II.2.a), truy cập vào máy tính WS2016 từ máy tính Window 7/8/10 bằng tài khoản này, sau đó tạo thử một số file trong thư mục này và kiểm tra xem các file này đã có trên thư mục trong máy WS2016 chưa. Cú pháp tài khoản: username = “MSSV”, Password tùy ý.

3. Triển khai dịch vụ Active Directory

a) Giới thiệu Workgroup

Khái niệm: Workgroup là một kiểu tổ chức mạng trong đó các máy tính được kết nối với nhau trong cùng một mạng LAN (Local Area Network) và chia sẻ tài nguyên mà không có máy chủ trung tâm nào điều khiển. Trong một workgroup, mỗi máy tính được coi là đồng bộ và có trách nhiệm tự quản lý tài nguyên của mình.

Computer Workgroup Setup



Hình 32: Mô hình cài đặt mạng máy tính theo Workgroup

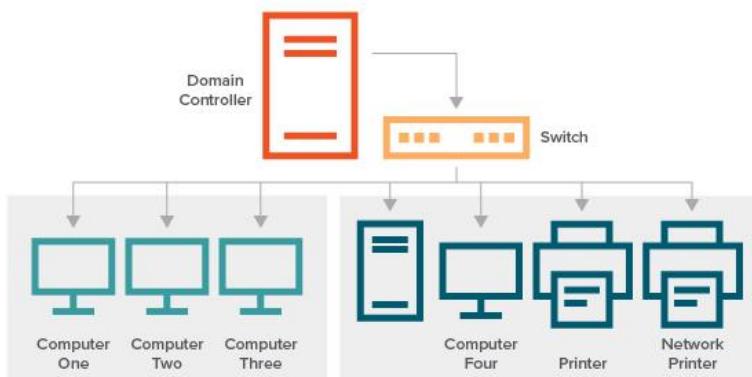
Workgroup có các đặc điểm sau:

- Tính phi tập trung: Trong một workgroup, không có máy chủ chung nào quản lý các máy tính khác. Mỗi máy tính hoạt động độc lập và tự quản lý tài nguyên của mình. Nghĩa là không có sự hoạch định về máy chủ và máy khách, mỗi máy tính hoạt động giống như máy khách cũng như máy chủ.
- Đơn giản và linh hoạt: Workgroup thường được triển khai trong các mạng nhỏ và đơn giản, không yêu cầu cấu hình phức tạp. Cài đặt và quản lý workgroup là dễ dàng và linh hoạt.
- Đăng nhập địa phương: Người dùng cần phải đăng nhập trực tiếp vào từng máy tính cụ thể trong workgroup để truy cập vào tài nguyên và dữ liệu.
- Chia sẻ tài nguyên: Các máy tính trong workgroup có thể chia sẻ tài nguyên như máy in, thư mục và tệp tin với các máy tính khác trong cùng một mạng.

b) Giới thiệu Domain Controller

Khái niệm:

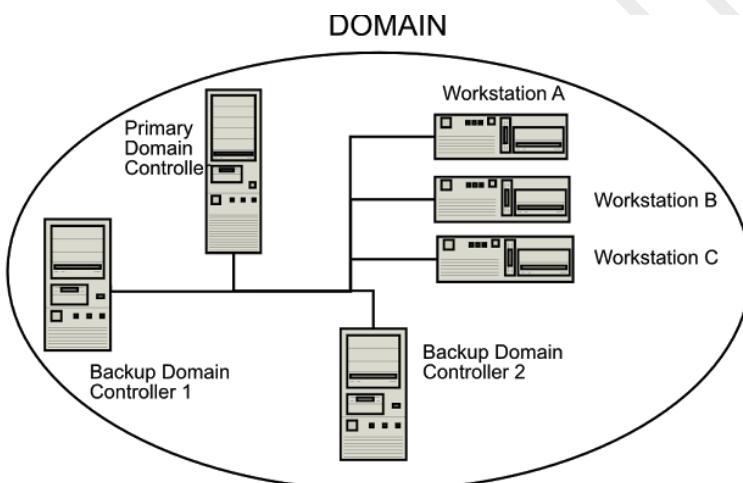
- **Domain** mô tả một hệ thống hay tập hợp những người dùng, các ứng dụng và máy chủ dữ liệu, hoặc thậm chí là bất kỳ loại tài nguyên nào được doanh nghiệp quan tâm, sử dụng. Tất cả chúng được quản lý trên một bộ quy tắc chung nào đó cùng những đặc điểm riêng.
- Thuật ngữ **Domain Controller** có nghĩa rộng hơn Domain. Nó dùng để chỉ hệ thống máy chủ sở hữu chức năng quản lý một Domain cụ thể nào đó. Một Domain thường có bản chất giống như một Server mà người dùng vẫn thường hay gặp. Nó chịu trách nhiệm quản lý an ninh mạng cũng như những vấn đề liên quan khác tới dữ liệu.



Hình 33: Mô hình cài đặt mạng máy tính theo Domain Controller

Phân loại Domain Controller:

- Primary Domain Controller hay PDC: Với loại này, mọi tài nguyên, hình ảnh, dữ liệu hay thông tin cần được bảo mật của Domain đều sẽ được lưu trữ cẩn thận. Việc lưu trữ diễn ra bên trong cơ sở dữ liệu ở các thư mục chính mà ở đây chính là Windows Server của cá nhân, công ty hay doanh nghiệp nào đó.
- Backup Domain Controller (BCD): Khi một PDC cũ bị lỗi hay có sự cố, vấn đề không thể hoạt động được nữa, thì một PDC mới sẽ được hình thành để tiếp nối. Nó đóng vai trò cân bằng lại khối lượng công việc, tự động sao chép cơ sở dữ liệu trong mỗi chu kỳ của BDC. Điều này nhằm mục đích đảm bảo an toàn, hạn chế tối đa những mất mát bên trong các thư mục chính.



Hình 34: Phân loại Domain Controller

Đặc điểm hoạt động Domain Controller:

- Quản lý tài khoản người dùng: Domain Controller lưu trữ thông tin về các tài khoản người dùng, bao gồm tên người dùng, mật khẩu, quyền truy cập và các thông tin khác liên quan.
- Quản lý tài nguyên mạng: Domain Controller quản lý và điều hành các tài nguyên mạng như máy in, máy chủ, ổ đĩa chia sẻ và các dịch vụ mạng khác.
- Xác thực truy cập: Domain Controller kiểm tra và xác thực các yêu cầu truy cập từ người dùng và máy tính trong mạng, đảm bảo rằng chỉ những người dùng được phép sử dụng các tài nguyên.
- Quản lý chính sách bảo mật: Domain Controller thiết lập và thực thi các chính sách bảo mật trên toàn bộ domain, bao gồm quy định về mật khẩu, quyền truy cập và các hạn chế khác.

c) Giới thiệu Active Directory

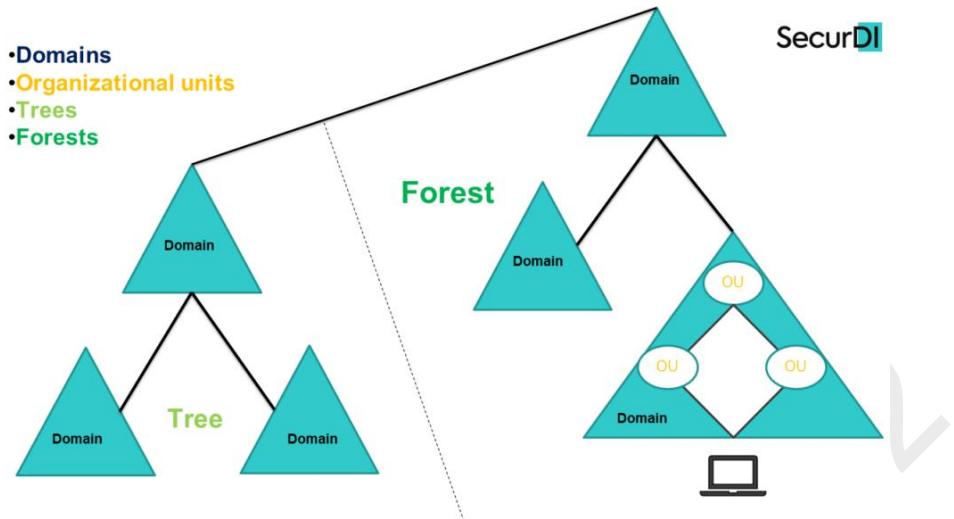
Khái niệm: Active Directory (AD) là một dịch vụ thư mục chạy trên Microsoft Windows Server, được gọi với tên gọi khác phổ biến hơn là Active Directory Domain Services (ADDS). Chức năng chính của Active Directory là cho phép các quản trị viên quản lý quyền hạn và kiểm soát truy cập vào các tài nguyên mạng. Trong Active Directory, dữ liệu được lưu trữ dưới dạng các đối tượng, bao gồm người dùng, nhóm, ứng dụng và thiết bị, và các đối tượng này được phân loại dựa trên tên và các thuộc tính của chúng. Khi dịch vụ Active Directory Domain Services được cài đặt trên một máy chủ, máy chủ đó trở thành một domain controller (DCs). Domain controller lưu trữ toàn bộ cơ sở dữ liệu AD, bao gồm các đối tượng, cây và mối quan hệ của chúng. Các tổ chức thường có nhiều domain controller, và mỗi domain controller đều có một bản sao của thư mục cho toàn bộ domain. Những thay đổi được thực hiện trên thư mục trên một domain controller, ví dụ như cập nhật mật khẩu hoặc thêm/xóa dữ liệu, sẽ được sao chép (replicate) đến các domain controller khác để đảm bảo rằng tất cả các domain controller đều cập nhật. Các máy tính để bàn, laptop và các thiết bị khác chạy hệ điều hành Windows (không phải Windows Server) có thể thuộc môi trường Active Directory, nhưng chúng không chạy dịch vụ Active Directory Domain Services.

Đặc điểm của AD:

- Tính bảo mật: mức độ bảo mật được cải thiện bằng cách kiểm soát quyền truy cập vào tài nguyên mạng.
- Tính mở rộng: là một quy trình đơn giản để các công ty dễ dàng tổ chức dữ liệu Active Directory để phù hợp với cơ cấu tổ chức và nhu cầu kinh doanh của họ.
- Tính đơn giản: quản trị viên hệ thống mạng có thể quản lý tập trung danh tính người dùng và đặc quyền truy cập trên toàn doanh nghiệp, từ đó giúp giảm chi phí hoạt động.
- Tính tự phục hồi: vì AD hỗ trợ các thành phần dự phòng và sao chép dữ liệu, nó tạo điều kiện cho hoạt động kinh doanh liên tục.

Kiến trúc hoạt động của AD:

- Domains: là một nhóm các đối tượng như người dùng, nhóm và thiết bị, chia sẻ cùng một cơ sở dữ liệu AD. Có thể hiểu domain như một nhánh trong cây.



Hình 35: Kiến trúc phân cấp của AD

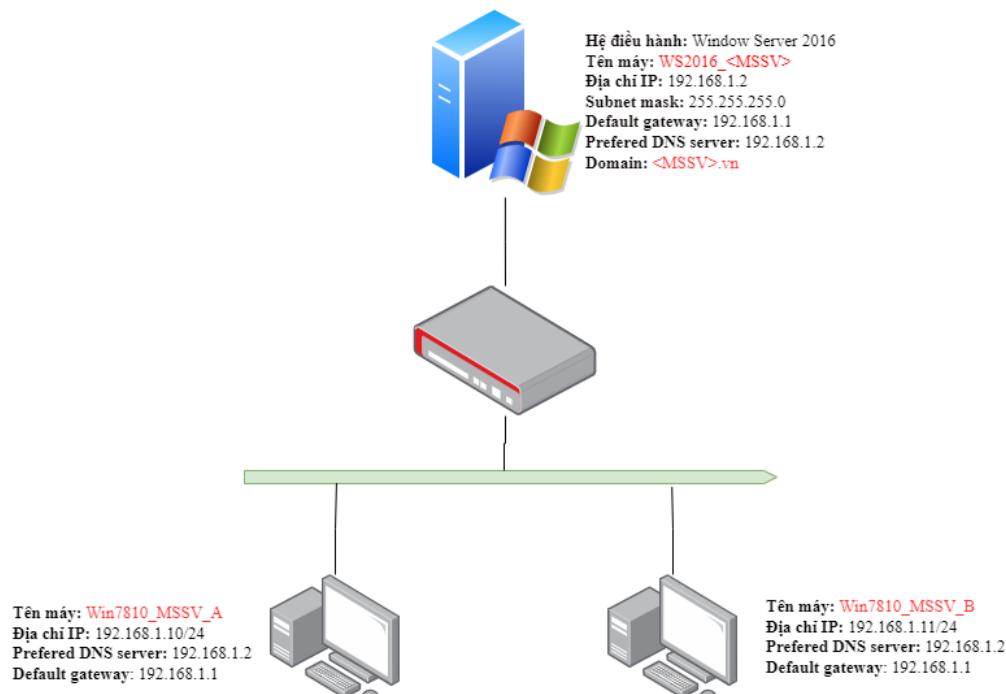
- **Trees:** Một tree là một hoặc nhiều domain được nhóm lại thành một cấu trúc phân cấp logic. Vì các domain trong một tree có mối quan hệ với nhau, chúng được gọi là "tin tưởng" nhau.
- **Forest:** Forest là cấp tổ chức cao nhất trong AD và chứa một nhóm các trees. Các trees trong một forest cũng có thể “tin tưởng” nhau và chia sẻ các schema, catalog, thông tin ứng dụng và cấu hình domain.
- **Organizational Units (OU):** Một OU được sử dụng để tổ chức người dùng, nhóm, máy tính và các đơn vị tổ chức khác.
- **Containers:** Một container tương tự như một OU, tuy nhiên, khác với OU, không thể liên kết một Group Policy Object (GPO) với một container Active Directory thông thường.

d) Cài đặt Active Directory trên WS2016

Một số tài liệu tham khảo có thể sử dụng ở giai đoạn này:

- [1] [Tài liệu tham khảo 1](#)
- [2] [Tài liệu tham khảo 2.1](#)
- [3] [Tài liệu tham khảo 2.2](#)

Trước khi cài đặt dịch vụ AD trên máy WS2016, sinh viên cần cài đặt sẵn trên máy ảo VMWare có 1 máy chạy WS2016 và 2 máy client Windows 7/8/10. Với máy chạy WS2016 thực hiện các bước cấu hình cho mỗi máy theo hướng dẫn trong mục II.1 và II.2 của tài liệu. Sơ đồ quan hệ và thông số của các máy phải được bố trí như hình 36.



Hình 36: Kiến trúc mạng máy tính cài đặt dịch vụ AD

Cài đặt dịch vụ AD trên máy chạy WS2016 theo hướng dẫn của:

- Tài liệu tham khảo 1: tham khảo từ trang 44 đến trang 52 (*khuyến khích chính*)
- Tài liệu tham khảo 2.1

e) Cấu hình dịch vụ AD trên WS2016

Tham khảo theo hướng dẫn của một trong các tài liệu dưới. Lưu ý ở bước cài đặt “Deployment Configuration” sinh viên cần đặt tên domain theo như mô tả trong hình 36.

- Tài liệu 1: tham khảo từ trang 53 đến trang 62.
- Tài liệu 2.2

III. Quy định bài thực hành

1. Sinh viên cần trình bày bài làm theo file template được GV cung cấp và nộp lại trên hệ thống LMS theo đúng deadline và các quy định liên quan.
2. Không chấp nhận những bài làm có dấu hiệu sao chép giống nhau và sẽ cho 0 điểm bài LAB của những bài làm này.

----HẾT----



I. Tóm tắt bài thực hành

1. Yêu cầu lý thuyết

Sinh viên đã được trang bị các kiến thức sau:

- Kiến trúc của hệ điều hành Windows Server.
- Các tính năng nổi bật của hệ điều hành Windows Server.
- Dịch vụ thư mục Active Directory.
- Quản trị Active Directory.
- ...

2. Nội dung chính bài thực hành

- Triển khai dịch vụ Active Directory.
 - Thực hiện join máy client vào domain của server.
 - Thêm một domain con vào cây domain hiện có.
 - Tạo và cấu hình tài khoản trên Domain Controller.
 - Tạo OU, Group, User và cấu hình ủy quyền quản trị OU.

Bảng 1: Bảng ánh xạ các giá trị liên quan

Gía trị trong tài liệu tham khảo 1	Gía trị ánh xạ tương ứng trong tài liệu thực hành	Ý nghĩa
BKAP-DC12-01	WS2016_<MSSV>	Tên máy chủ chạy WS2016
BKAP-WRK08-01	Win7810_<MSSV>_A	Tên máy client chạy Window 7/8/10
BKAP-WRK08-02	Win7810_<MSSV>_B	Tên máy client chạy Window 7/8/10
BKAP-SRV12-01	SUB_WS2016_<MSSV>	Tên máy con chạy WS2016
bkaptech.vn.	<MSSV>.vn	Tên domain
duynh	<MSSV>us1 <ul style="list-style-type: none"> • First name: <MSSV> • Last name: us1 • Full name: <MSSV>us1 	Thông tin tài khoản của user

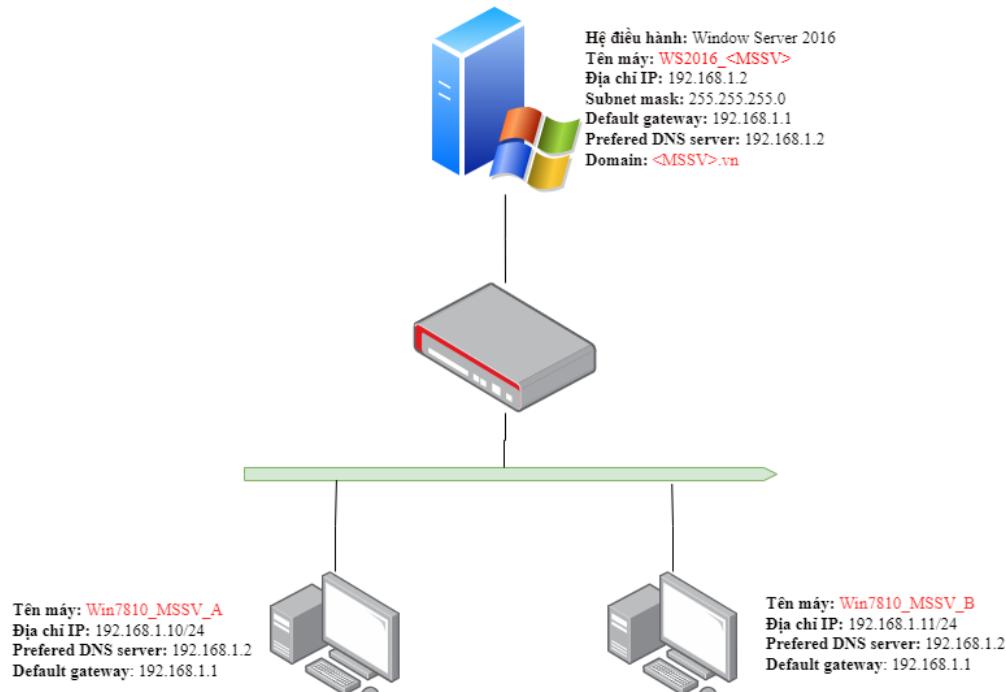
	<ul style="list-style-type: none"> • User logon name: <MSSV>us1 (@<MSSV>.vn) • Password: 123456a@ 	
hungnq	<MSSV>us2 // Xử lý thông tin tài khoản user tương tự như trên.	
cuongvv	<MSSV>us3 // Xử lý thông tin tài khoản user tương tự như trên.	
quanch	<MSSV>us4 // Xử lý thông tin tài khoản user tương tự như trên	
truonglv	<MSSV>us5 // Xử lý thông tin tài khoản user tương tự như trên	
nghialv	<MSSV>us6 // Xử lý thông tin tài khoản user tương tự như trên	
cuongnt	<MSSV>us7 // Xử lý thông tin tài khoản user tương tự như trên	
cuongvv	<MSSV>us8 // Xử lý thông tin tài khoản user tương tự như trên	

II. Chi tiết bài thực hành

1. Thực hiện join máy client vào domain của server

Ở bài LAB1, sinh viên đã hoàn thành việc tạo một mô hình mạng máy tính gồm 1 máy chạy WS2016 và 2 máy client chạy Window 7/8/10 với các thông số (địa chỉ IP, Preferred DNS...) tương ứng. Kiến trúc mô hình được mô tả như hình 1.

Để thực hiện yêu cầu trong phần này, SV chọn 1 trong 2 máy client đã cài đặt trên VMWare sau đó tham khảo các bước thực hiện từ trang 63 đến trang 70 của [Tài liệu tham khảo 1](#). Lưu ý cần cù hính các tham số cho tương ứng như hình 1 sau khi tham chiếu từ tài liệu tham khảo 1 (có thể tham khảo thêm bảng 1) và cần đảm bảo trước máy chủ chạy WS2016 đã được nâng cấp thành Domain Controller (tham khảo LAB1).



Hình 1: Kiến trúc mạng máy tính cho nội dung thực hành 1

2. Thêm một domain con vào cây domain hiện có

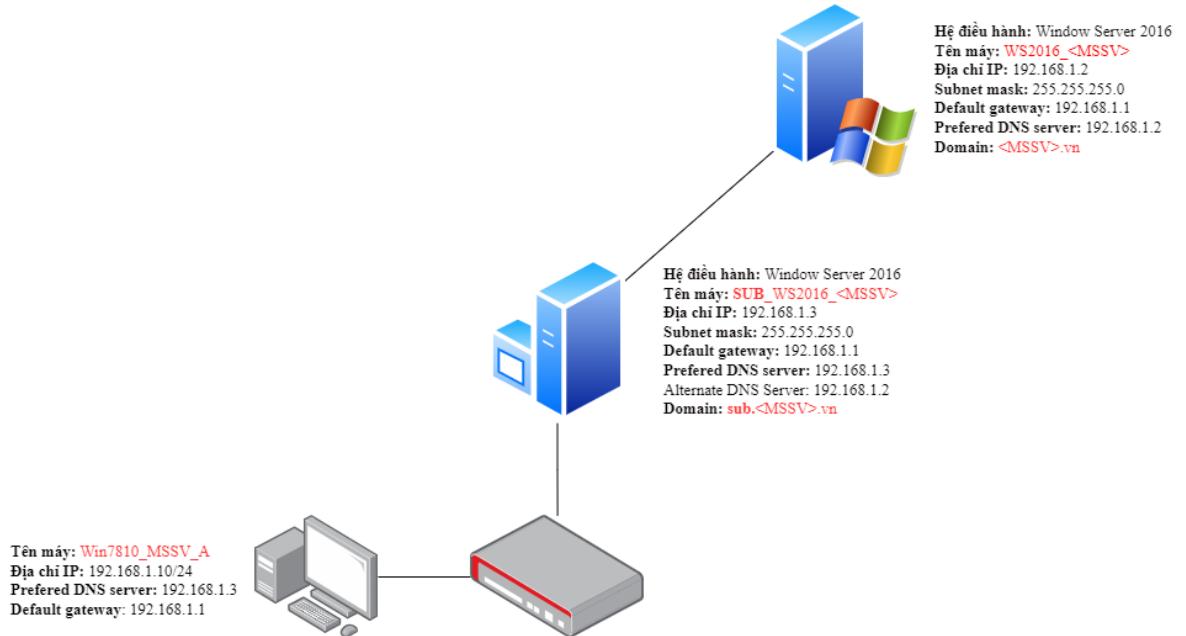
Thêm child domain vào cây domain hiện có là quá trình tạo ra một domain mới dưới một domain cha (parent domain) đã tồn tại trong cấu trúc AD. Quá trình này tạo ra một mối quan hệ phân cấp giữa các domain, với domain cha là một mức cao hơn và domain con là một mức thấp hơn trong cấu trúc. Mục đích của việc làm này bao gồm phân chia sự quản lý của các đơn vị tổ chức, phòng ban hoặc chi nhánh khác nhau trong một tổ chức lớn, tối ưu hóa hiệu suất hệ thống, cải thiện bảo mật thông qua triển khai các chính sách bảo mật riêng biệt, và khả năng mở rộng khi tổ chức phát triển và mở rộng. Sinh viên thực hành nội dung này theo các bước như sau:

Bước 1: Cài đặt thêm một máy chạy WS2016 đặt tên theo cú pháp **SUB_WS2016_<MSSV>** trên VMWare.

Bước 2: Xem xét kiến trúc mạng máy tính thiết lập ở hình 2.

Bước 3: SV chọn 1 trong 2 máy client đã cài đặt trên VMWare sau đó tham khảo các bước thực hiện từ trang 107 đến trang 121 của [Tài liệu tham khảo 1](#). Lưu ý cấu hình

các thông số cho tương ứng như hình 2 sau khi tham chiếu từ tài liệu tham khảo 1 hoặc bảng 1.



Hình 2: Kiến trúc mạng máy tính cho nội dung thực hành 2

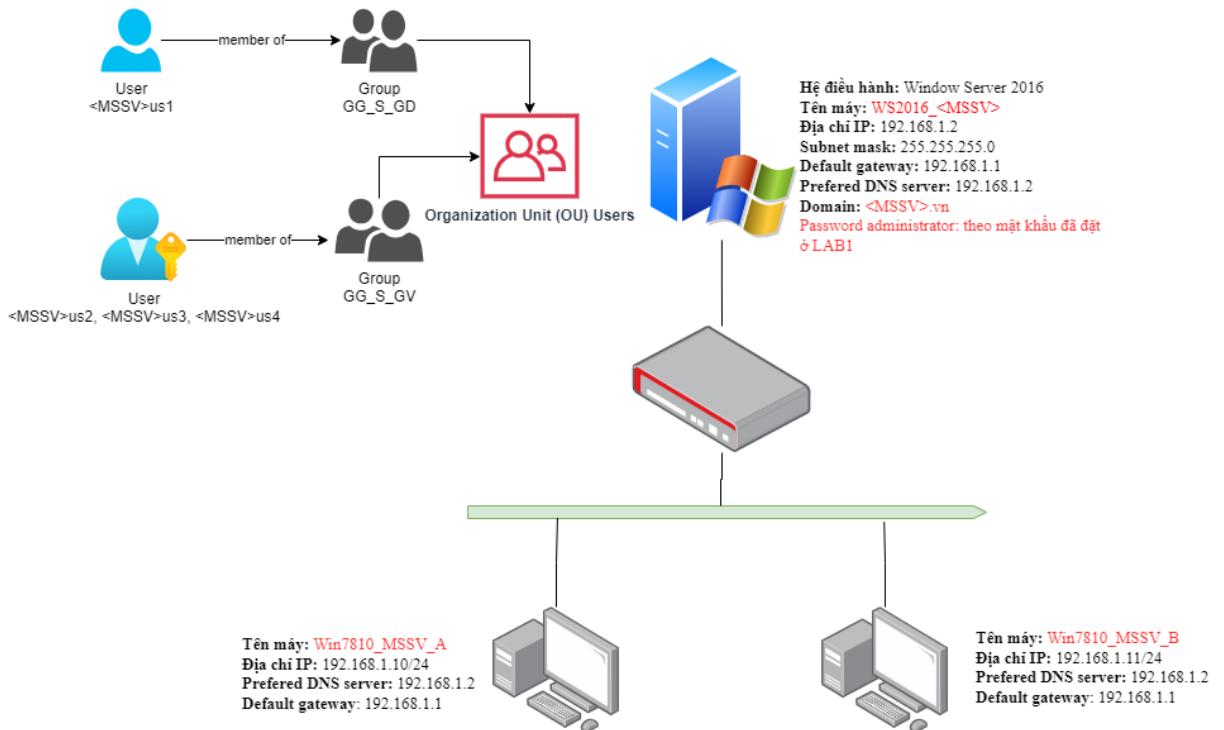
3. Tạo và cấu hình tài khoản trên Domain Controller

Tạo và cấu hình tài khoản người dùng trên Domain Controller là quan trọng để quản lý và kiểm soát quyền truy cập vào các tài nguyên mạng trong một môi trường Active Directory. Bằng cách này, quản trị viên có thể tạo ra và quản lý các tài khoản người dùng một cách tập trung, đồng thời thiết lập các chính sách bảo mật, quyền truy cập và cấu hình đối với từng người dùng. Việc tạo và cấu hình tài khoản người dùng trên Domain Controller cũng đảm bảo tính nhất quán và an toàn của hệ thống, giúp quản trị viên dễ dàng theo dõi và kiểm soát quyền truy cập, đồng thời tăng cường bảo mật cho mạng máy tính.

Để thực hành nội dung này sinh viên thực hiện theo các bước được hướng dẫn chi tiết như trong [Tài liệu tham khảo 1](#) (trang 124 – 149) hoặc tham khảo tại [đây](#).

Một số lưu ý cho sinh viên:

- Phải thực hiện các bước dựa theo thông tin và các thông số cài đặt được thể hiện như trên hình 3.
- Khi tham khảo theo [Tài liệu tham khảo 1](#), sinh viên cần phải ánh xạ lại cho đúng từ các thông số cài đặt trong tài liệu tham khảo sang các thông số được minh họa trên hình 3 (thông tin user, địa chỉ IP,...). Sinh viên có thể tham khảo bảng 1 để nắm rõ hơn yêu cầu.

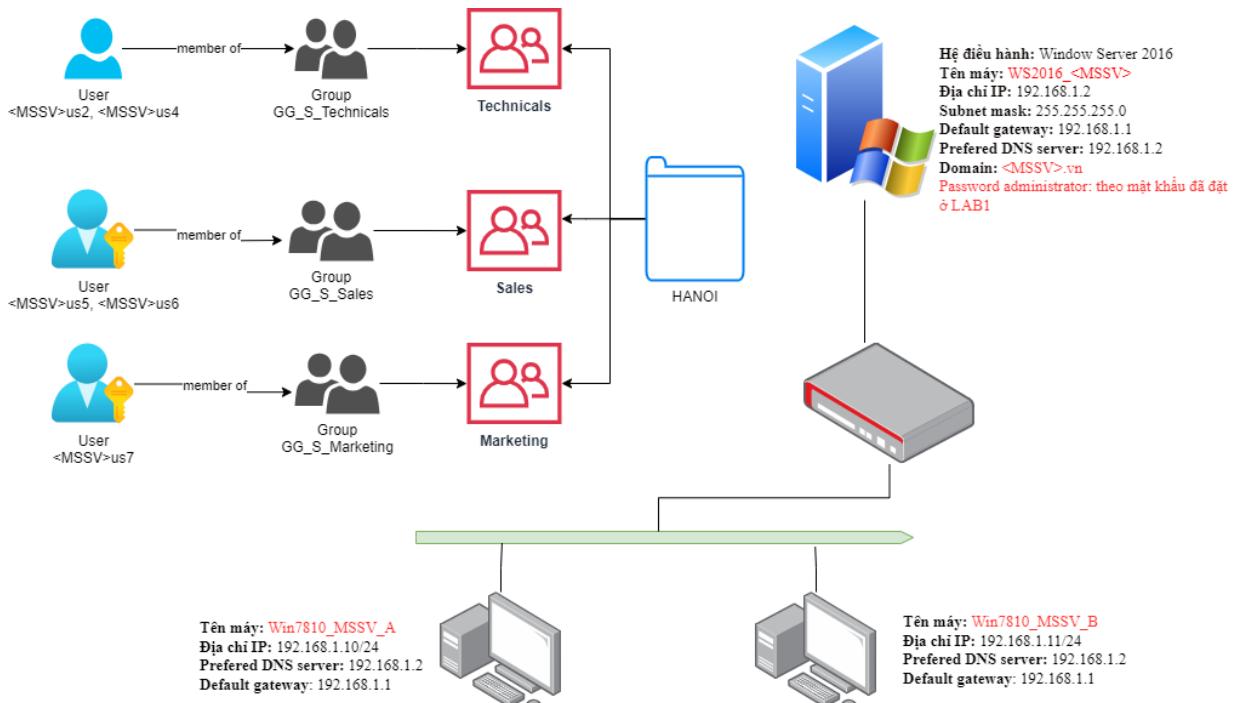


Hình 3: Kiến trúc mạng máy tính cho nội dung thực hành 3

4. Tạo OU, Group, User và cấu hình ủy quyền quản trị OU trên Domain Controller

Việc tạo Organizational Units (OU), nhóm (Group), người dùng (User) và cấu hình ủy quyền quản trị OU trên Domain Controller là quan trọng để tổ chức và quản lý hiệu quả bằng dịch vụ AD. OU được sử dụng để tổ chức và phân loại người dùng, nhóm và các đơn vị tổ chức khác theo cách logic và phản ánh cấu trúc hoạt động của tổ chức. Nhóm được sử dụng để quản lý quyền truy cập và phân quyền cho người dùng vào các tài nguyên trong mạng. Người dùng được tạo ra để xác định và quản lý các tài khoản người dùng trên hệ thống. Cấu hình ủy quyền quản trị OU trên Domain Controller là cần thiết để phân quyền cho quản trị viên và người dùng khác trong tổ chức, giúp họ có thể quản lý và thực hiện các thao tác như thêm, sửa đổi hoặc xóa các đối tượng trong OU một cách an toàn và hiệu quả. Việc này giúp tăng cường bảo mật và quản lý, đồng thời đảm bảo rằng chỉ các người dùng được ủy quyền mới có thể thực hiện các hoạt động quản trị trên hệ thống.

Để hoàn thành nội dung này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 1](#) trang 150-176. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 4.



Hình 4: Kiến trúc mạng máy tính cho nội dung thực hành 4

III. Quy định bài thực hành

- Sinh viên cần trình bày bài làm theo file template được GV cung cấp.
- Nộp lại trên hệ thống LMS theo đúng deadline và các quy định liên quan.
- Không chấp nhận những bài làm có dấu hiệu sao chép giống nhau và sẽ cho 0 điểm bài LAB của những bài làm này.

----HẾT----



I. Tóm tắt bài thực hành

1. Yêu cầu lý thuyết

Sinh viên đã được trang bị các kiến thức về dịch vụ DHCP và dịch vụ AD.

2. Nội dung chính bài thực hành

- o Cài đặt và cấu hình quản lý DHCP Server kết hợp với AD.
- o Cài đặt và cấu hình DHCP Relay Agent.
- o Sao lưu và khôi phục DHCP Server.
- o Cài đặt và cấu hình DHCP Failover.

Bảng 1: Bảng ánh xạ các giá trị liên quan

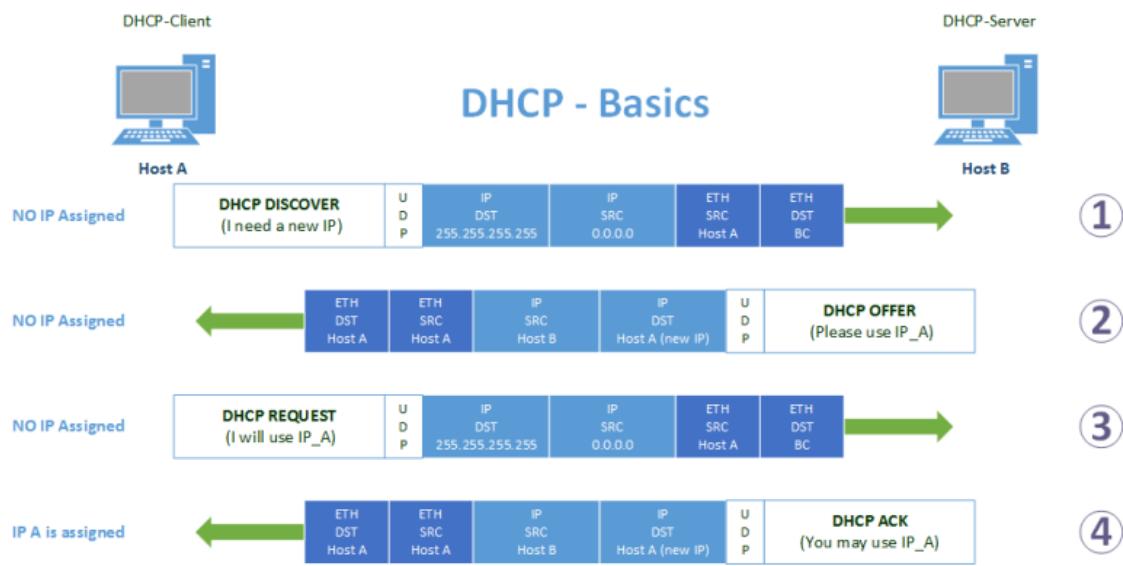
Gía trị trong tài liệu tham khảo 1	Gía trị ánh xạ tương ứng trong tài liệu thực hành	Ý nghĩa
BKAP-DC12-01	WS2016_<MSV>	Tên máy chủ thứ nhất chạy WS2016
BKAP-SRV12-01	ALT_WS2016_<MSV>	Tên máy chủ thứ hai chạy WS2016
bkaptech.vn.	<MSV>.vn	Tên domain
BKAP-WRK08-01	Win7810_<MSV>_C	Tên máy client thứ nhất chạy Window 7/8/10
BKAP-WRK08-02	Win7810_<MSV>_D	Tên máy client thứ hai chạy Window 7/8/10

II. Chi tiết bài thực hành

1. Cài đặt và cấu hình quản lý DHCP Server kết hợp với AD

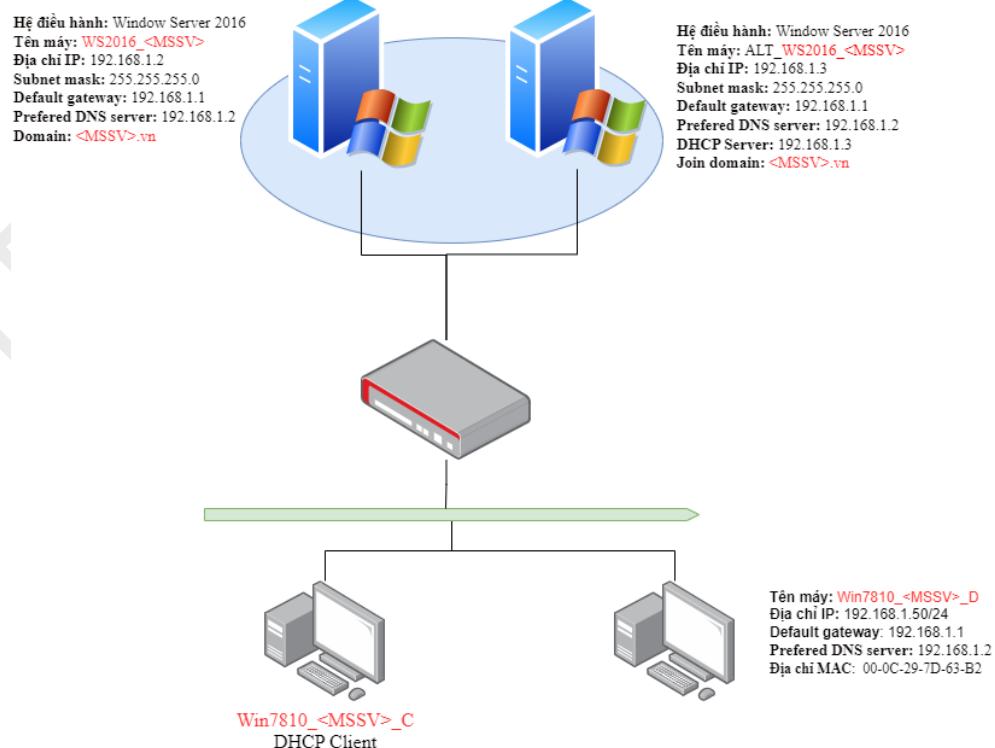
Dịch vụ DHCP (Dynamic Host Configuration Protocol) là một dịch vụ trong mạng máy tính giúp tự động cấu hình các thiết bị mạng để có thể kết nối và tham gia vào mạng một cách dễ dàng và tự động. DHCP server là máy chủ chịu trách nhiệm phân phối các thông tin cấu hình IP (địa chỉ IP, subnet mask, default gateway, DNS server) cho các thiết bị mạng trong mạng LAN.

Ví dụ: Giả sử bạn có một mạng nội bộ trong văn phòng của mình. Bạn cài đặt một DHCP server trên mạng của mình. Khi một thiết bị mới (như một máy tính hoặc điện



Hình 1: Luồng hoạt động của DHCP Server trong mạng máy tính

thoại thông minh) kết nối vào mạng, nó sẽ gửi yêu cầu DHCP (DHCP request) để yêu cầu một địa chỉ IP và các thông tin cấu hình khác. DHCP server sẽ phản hồi lại bằng cách cấp cho thiết bị đó một địa chỉ IP, subnet mask, default gateway và thông tin DNS server. Khi đó, thiết bị sẽ tự động cấu hình các thông tin này và có thể truy cập vào mạng LAN mà không cần phải thủ công cấu hình. Điều này giúp tiết kiệm thời gian và giảm thiểu lỗi cấu hình trong môi trường mạng lớn.

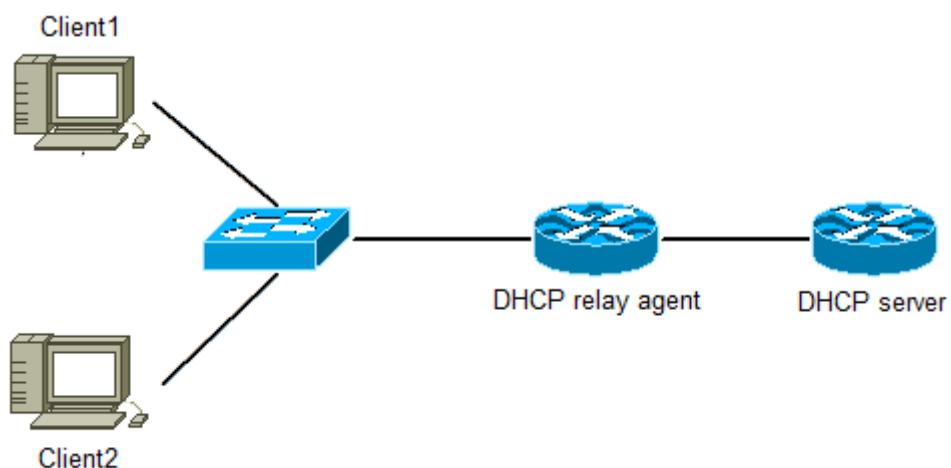


Hình 2: Kiến trúc mạng máy tính cho nội dung thực hành 1

Để thực hành nội dung này, sinh viên tạo hai máy client mới chạy Window 7/8/10 tên Win7810_< MSSV >_C và Win7810_< MSSV >_D sau đó thực hiện theo các bước hướng dẫn và đạt yêu cầu đầu ra theo [Tài liệu tham khảo 1](#) (từ trang 203 - 221). **Dòng thời nội dung thực hành phải dựa trên bảng ánh xạ giá trị từ tài liệu tham khảo (bảng 1) và theo kiến trúc mạng được minh họa trên hình 2.**

2. Cài đặt và cấu hình DHCP Relay Agent.

DHCP Relay Agent (Đại lý chuyển tiếp DHCP) là một thiết bị hoặc phần mềm được sử dụng để chuyển tiếp các yêu cầu DHCP giữa các máy khách (clients) và máy chủ DHCP (server) trên các mạng khác nhau. Thông thường, trong một mạng máy tính lớn hoặc phân tán, các máy khách DHCP có thể nằm trên các mạng con khác nhau và không thể liên lạc trực tiếp với máy chủ DHCP do các giới hạn về phạm vi phát sóng (broadcast domain). DHCP Relay Agent giúp giải quyết vấn đề này bằng cách chuyển tiếp các thông điệp DHCP giữa các máy khách và máy chủ qua các mạng khác nhau.

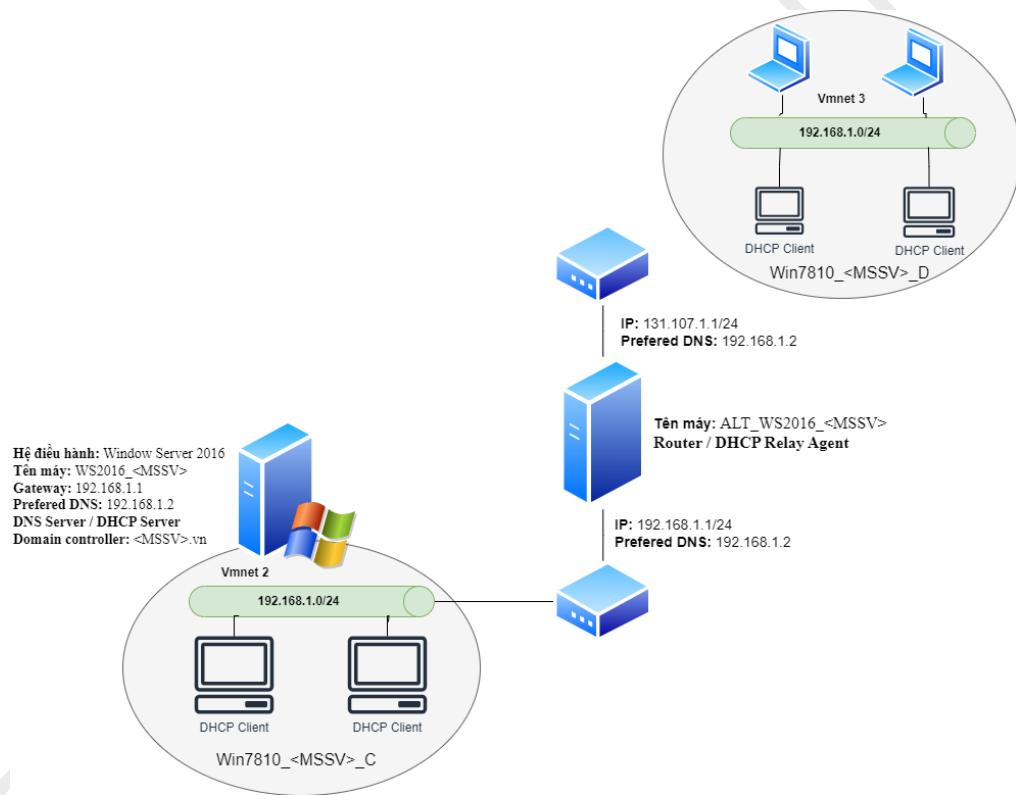


Hình 3: DHCP Relay Agent trong mạng máy tính

Ví dụ: Giả sử bạn có một tổ chức mạng với ba mạng con: Mạng A (192.168.1.0/24), Mạng B (192.168.2.0/24), và Mạng C (192.168.3.0/24). Máy chủ DHCP được đặt tại mạng A và không thể gửi các gói tin phát sóng trực tiếp tới các máy khách trong mạng B và C. Để giải quyết vấn đề này, bạn cấu hình một router hoặc thiết bị mạng khác ở mỗi mạng con B và C làm DHCP Relay Agent. Trên router của mạng B, bạn cấu hình để chuyển tiếp các yêu cầu DHCP đến địa chỉ IP của máy chủ DHCP tại mạng A. Tương tự, trên router của mạng C, bạn cũng cấu hình để chuyển tiếp các yêu cầu DHCP đến địa chỉ IP của máy chủ DHCP tại mạng A. Khi một máy khách trong mạng B (ví dụ: 192.168.2.10) gửi một yêu cầu DHCP (DHCP Discover), yêu cầu này được gửi đến router của mạng B, router này sẽ đóng gói yêu cầu DHCP và gửi nó

dưới dạng unicast đến máy chủ DHCP tại mạng A. Máy chủ DHCP nhận được yêu cầu, xử lý và gửi lại phản hồi (DHCP Offer) trở lại router của mạng B, và router mạng B sau đó sẽ chuyển tiếp phản hồi này tới máy khách ban đầu tại mạng B. Bằng cách này, DHCP Relay Agent cho phép các máy khách trong mạng B và C nhận được cấu hình IP từ máy chủ DHCP trung tâm tại mạng A, đảm bảo sự liên thông và quản lý hiệu quả giữa các mạng con khác nhau trong tổ chức.

Để thực hành nội dung này, sinh viên thực hiện theo các bước hướng dẫn và đạt yêu cầu đầu ra theo [Tài liệu tham khảo 1](#) (từ trang 221 - 246). *Đồng thời nội dung thực hành phải dựa theo kiến trúc mạng được minh họa trên hình 4 và chú ý ánh xạ các giá trị liên quan như trong bảng 1.*



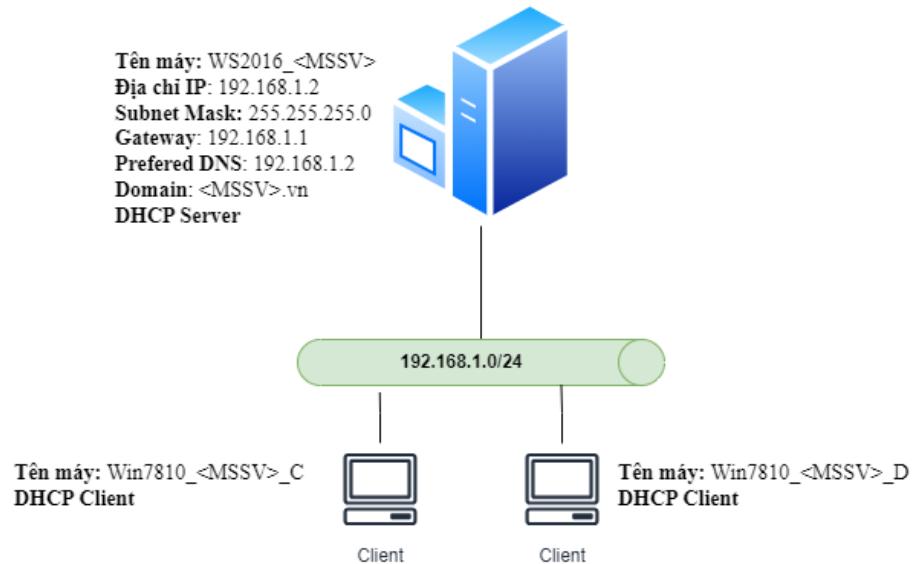
Hình 4: Kiến trúc mạng máy tính cho nội dung thực hành 2

3. Sao lưu và khôi phục DHCP server

Sao lưu và khôi phục DHCP server trên Windows Server là quá trình tạo bản sao và phục hồi dữ liệu đã cấu hình truy cập mạng cho các thiết bị và máy chủ trong cùng một môi trường mạng LAN cùng cơ sở dữ liệu của DHCP server nhằm đảm bảo tính liên tục của dịch vụ mạng, bảo vệ dữ liệu và tiết kiệm thời gian. Sao lưu giúp bảo vệ các cấu hình quan trọng tránh mất mát do sự cố không mong muốn, trong khi khôi phục cho phép nhanh chóng đưa dịch vụ trở lại hoạt động khi gặp sự cố. Thao tác này

thường được thực hiện trước khi nâng cấp hệ điều hành, cập nhật phần mềm, thay đổi cấu hình lớn, định kỳ hoặc sau mỗi thay đổi quan trọng.

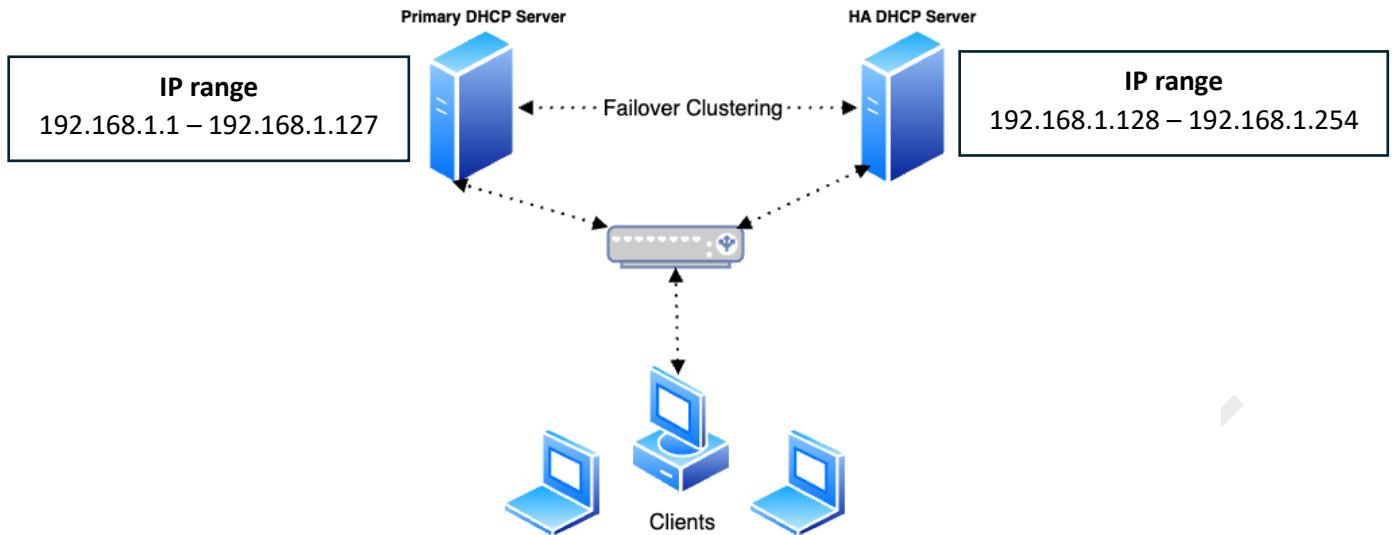
Để thực hành nội dung này, sinh viên thực hiện theo các bước hướng dẫn và đạt yêu cầu đầu ra theo [Tài liệu tham khảo 1](#) (từ trang 247 - 257). *Đồng thời nội dung thực hành phải dựa theo kiến trúc mạng được minh họa trên hình 7 của Tài liệu tham khảo 1 và chú ý ánh xạ các giá trị liên quan như trong bảng 1.*



Hình 7: Kiến trúc mạng máy tính cho nội dung thực hành 4

4. Cài đặt và cấu hình DHCP Failover.

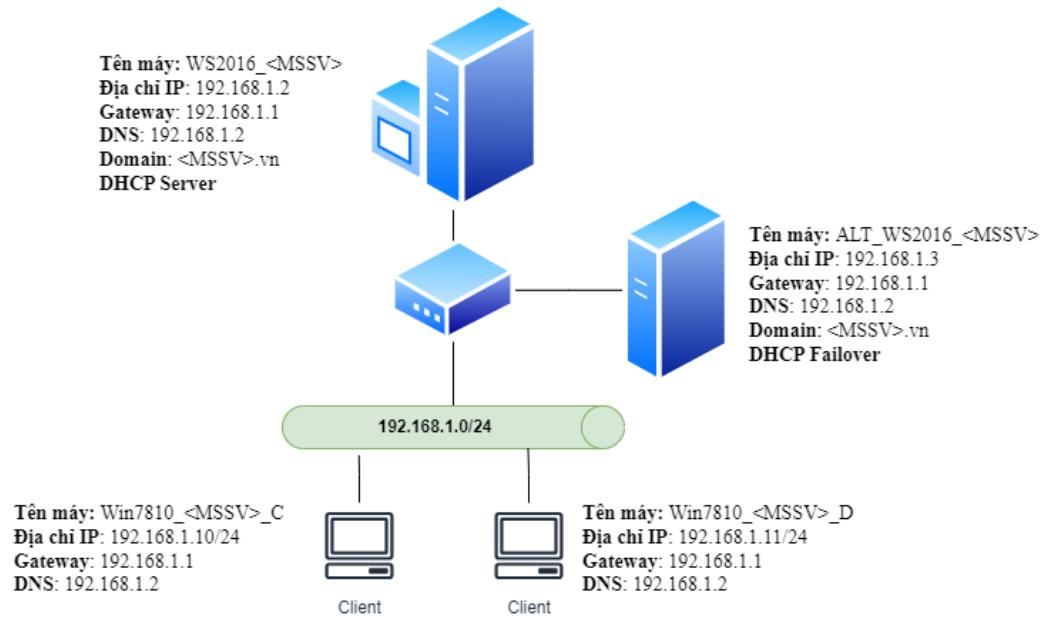
DHCP Failover là một cơ chế được thiết kế để đảm bảo tính liên tục và độ tin cậy của dịch vụ DHCP (Dynamic Host Configuration Protocol). DHCP Failover cho phép hai máy chủ DHCP hoạt động cùng nhau, chia sẻ gánh nặng và dự phòng cho nhau trong trường hợp một máy chủ gặp sự cố. Điều này đảm bảo rằng các thiết bị trên mạng vẫn có thể nhận được địa chỉ IP ngay cả khi một trong các máy chủ DHCP bị lỗi.



Hình 5: Kiến trúc hoạt động của DHCP Failover.

Ví dụ: Giả sử một công ty có hai máy chủ DHCP, *Primary DHCP Server* và *HA DHCP Server*, được cấu hình theo mô hình DHCP Failover để đảm bảo tính sẵn sàng cao và cân bằng tải. Cả hai máy chủ này chia sẻ một phạm vi địa chỉ IP, với *Primary DHCP Server* quản lý 50% địa chỉ IP đầu tiên và *HA DHCP Server* quản lý 50% địa chỉ IP còn lại. Khi một máy khách yêu cầu địa chỉ IP, yêu cầu này sẽ được xử lý bởi một trong hai máy chủ, ví dụ, máy chủ *Primary DHCP Server* sẽ cấp phát một địa chỉ IP từ phạm vi của nó và thông báo cho máy chủ *HA DHCP Server* để đồng bộ hóa thông tin. Nếu máy chủ *Primary DHCP Server* gặp sự cố và ngừng hoạt động, máy chủ *HA DHCP Server* sẽ tự động tiếp quản nhiệm vụ cấp phát địa chỉ IP cho các máy khách mới, đảm bảo rằng không có sự gián đoạn trong việc cấp phát địa chỉ IP và duy trì kết nối mạng liên tục.

Để thực hành nội dung này, sinh viên thực hiện theo các bước hướng dẫn và đạt yêu cầu đầu ra theo [Tài liệu tham khảo 4](#) (từ trang 3 - 21). Đồng thời nội dung thực hành phải dựa theo kiến trúc mạng được minh họa trên hình 6 và chú ý ánh xạ các giá trị liên quan như trong bảng 1.



Hình 6: Kiến trúc mạng máy tính cho nội dung thực hành 3

III. Quy định bài thực hành

1. Sinh viên cần trình bày bài làm theo file template được GV cung cấp.
2. Nộp lại trên hệ thống LMS theo đúng deadline và các quy định liên quan.
3. Không chấp nhận những bài làm có dấu hiệu sao chép giống nhau và sẽ cho 0 điểm bài LAB của những bài làm này.

----HẾT----



I. Tóm tắt bài thực hành

1. Yêu cầu lý thuyết

Sinh viên đã được trang bị các kiến thức về:

- Cài đặt và cấu hình dịch vụ DNS.
- Phân quyền và chia sẻ dữ liệu.
- Triển khai chính sách Group Policy.

2. Nội dung chính bài thực hành

- Cài đặt và cấu hình DNS Server.
- Cấu hình dịch vụ Backup DNS.
- Cấu hình và phân quyền chia sẻ dữ liệu.
- Cấu hình Offline Files.
- Triển khai chính sách GPO cơ bản.
- Giám sát tệp tin và bắt xóa file.

Bảng 1: Bảng ánh xạ các giá trị liên quan

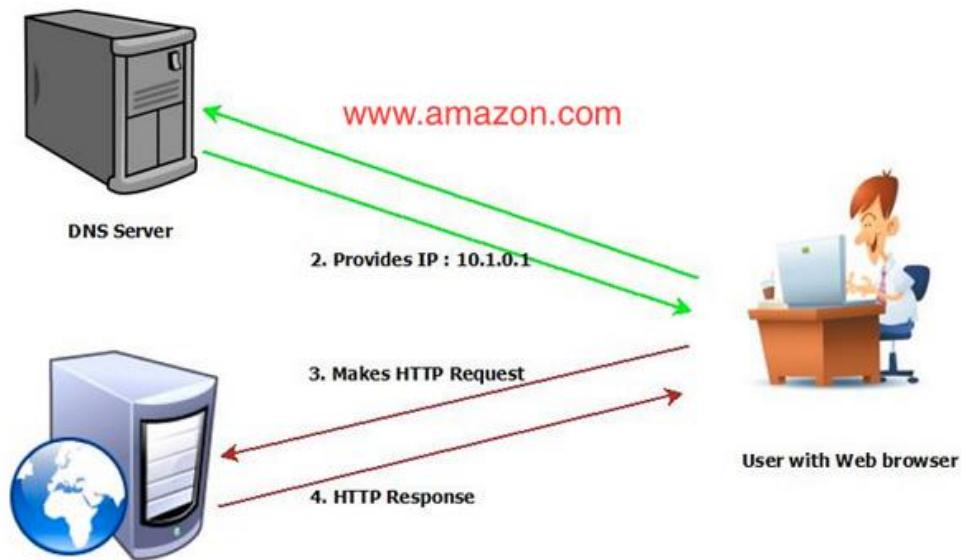
Gía trị trong tài liệu tham khảo 1	Gía trị ánh xạ tương ứng trong tài liệu thực hành	Ý nghĩa
BKAP-DC12-01	WS2016_<MSSV>	Tên máy chủ chính chạy WS2016
BKAP-SRV12-01	ALT_WS2016_<MSSV>	Tên máy chủ phụ thứ nhất chạy WS2016
BKAP-SRV-12-02	ALT2_WS2016_<MSSV>	Tên máy chủ phụ thứ hai chạy WS2016
BKAP-SRV-12-03	ALT3_WS2016_<MSSV>	Tên máy chủ phụ thứ ba chạy WS2016
bkaptech.vn.	<MSSV>.vn	Tên domain
BKAP-WRK08-01	Win7810_<MSSV>_C	Tên máy client thứ nhất chạy Window 7/8/10
BKAP-WRK08-02	Win7810_<MSSV>_D	Tên máy client thứ hai chạy Window 7/8/10

Thư mục IT	IT_<MSSV>	Thư mục IT tương ứng trên máy ALT_WS2016_<MSSV>
Thư mục Sale	Sale_<MSSV>	Thư mục Sale tương ứng trên máy ALT_WS2016_<MSSV>
Group GG_S_IT	GG_S_IT_<MSSV>	
Group GG_S_Sale	GG_S_Sale_<MSSV>	
hungnq	<MSSV>us2 <ul style="list-style-type: none"> • First name: <MSSV> • Last name: us2 • Full name: <MSSV>us2 • User logon name: <MSSV>us2 (@<MSSV>.vn) • Password: 123456a@ 	
nghialv	<MSSV>us6 <p>// Xử lý thông tin tài khoản user tương tự như trên</p>	

II. Chi tiết bài thực hành

1. Cài đặt và cấu hình DNS Server.

DNS (Domain Name System) server là một thành phần quan trọng trong hệ thống mạng internet. Nó hoạt động như một danh bạ điện thoại của internet, chuyển đổi các tên miền dễ nhớ như www.example.com thành các địa chỉ IP dạng số như 192.168.1.1 mà máy tính sử dụng để xác định lẫn nhau trên mạng. Khi người dùng nhập một tên miền vào trình duyệt, yêu cầu này được gửi đến một máy chủ DNS, nơi nó được tra cứu để tìm ra địa chỉ IP tương ứng. Điều này không chỉ giúp cải thiện trải nghiệm người dùng mà còn tối ưu hóa hiệu suất mạng bằng cách lưu trữ tạm thời (caching) các bản ghi DNS, giảm thời gian cần thiết để tìm kiếm địa chỉ IP cho các yêu cầu lặp lại. Ngoài ra, máy chủ DNS còn đóng vai trò quan trọng trong việc bảo mật, ngăn chặn các truy cập độc hại và điều hướng người dùng đến các nguồn tài nguyên chính xác và an toàn.

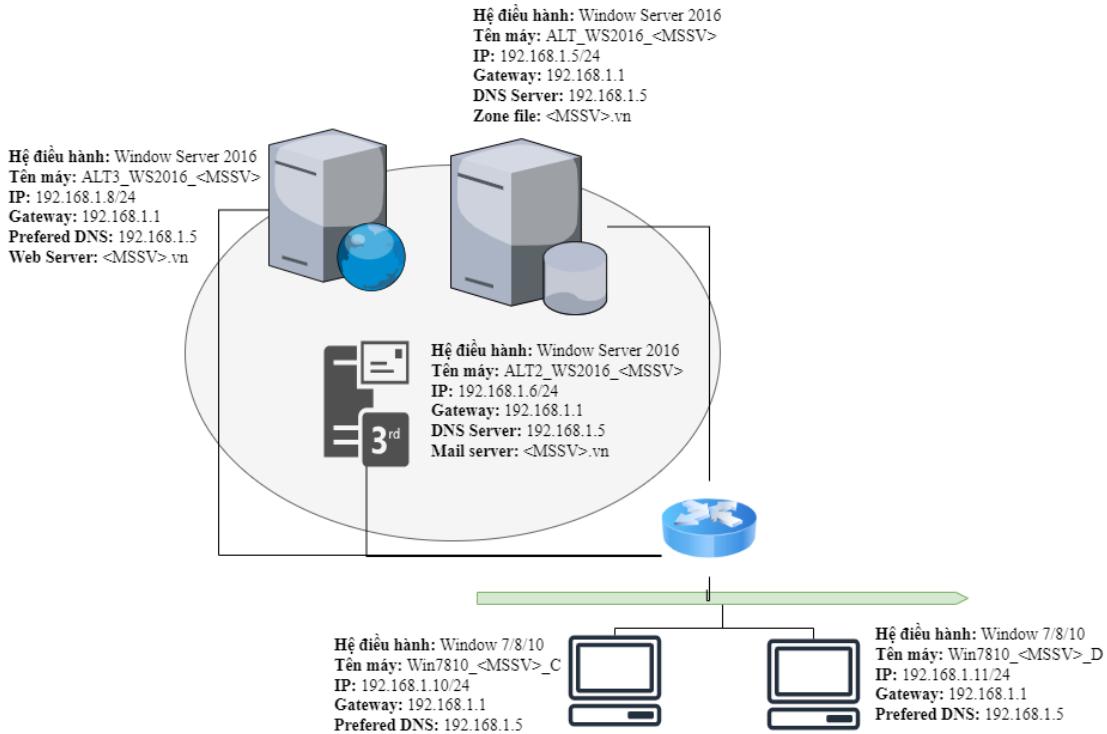


Hình 1: Minh họa nguyên lý hoạt động của DNS Server

Ví dụ bạn muốn truy cập trang web www.amazon.com. Khi bạn nhập tên miền này vào trình duyệt, máy tính của bạn không tự động biết được địa chỉ IP của trang web. Thay vào đó, yêu cầu truy cập được gửi đến máy chủ DNS. Máy chủ DNS sau đó sẽ tra cứu tên miền www.amazon.com trong cơ sở dữ liệu của nó để tìm ra địa chỉ IP tương ứng, chẳng hạn như 10.1.0.1. Sau khi xác định được địa chỉ IP, máy chủ DNS sẽ gửi lại thông tin này cho trình duyệt của bạn, cho phép nó kết nối đến máy chủ lưu trữ trang web và hiển thị nội dung cho bạn.

Trong Windows Server, DNS Server là một dịch vụ quan trọng, chịu trách nhiệm quản lý và cung cấp các dịch vụ phân giải tên miền trong mạng nội bộ. Khi một máy tính trong mạng cần biết địa chỉ IP của một tên miền cụ thể, nó sẽ gửi yêu cầu đến máy chủ DNS. Máy chủ DNS sẽ kiểm tra bộ nhớ đệm (cache) của nó trước để xem liệu địa chỉ IP của tên miền đã được lưu trữ từ trước hay chưa tương ứng với tên miền được yêu cầu. Nếu có, nó sẽ trả về kết quả ngay lập tức. Nếu không, máy chủ DNS sẽ tiếp tục tìm kiếm trong cơ sở dữ liệu vùng (zone files) mà nó quản lý. Nếu tên miền không nằm trong cơ sở dữ liệu vùng của nó, DNS server của Windows Server sẽ gửi truy vấn đến các máy chủ DNS khác trên internet, bắt đầu từ các máy chủ gốc (root servers). Quá trình này tiếp tục cho đến khi tìm được địa chỉ IP chính xác, sau đó kết quả được trả về cho máy tính yêu cầu.

DNS Server trong Windows Server thường được cấu hình với các khu vực (zones), mỗi khu vực đại diện cho một tên miền cụ thể hoặc một phần của không gian tên miền.



Hình 2: Kiến trúc mạng máy tính cho nội dung thực hành 1

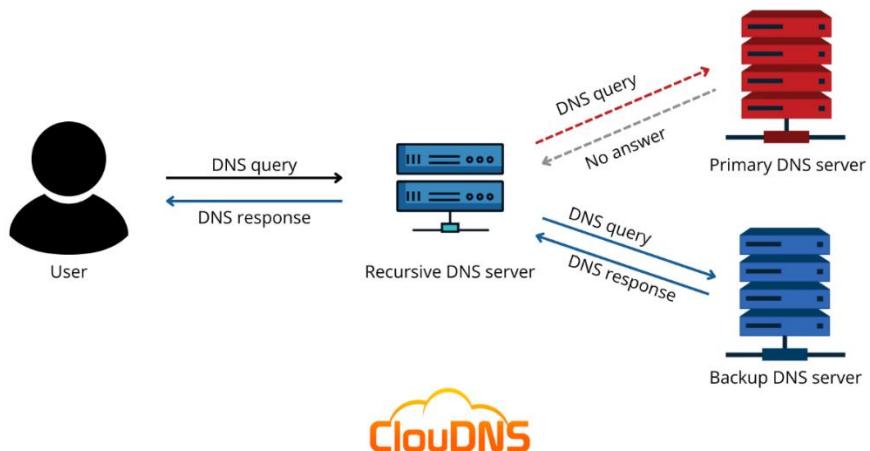
Trong mỗi khu vực, DNS Server lưu trữ các bản ghi (records) DNS, bao gồm bản ghi A (địa chỉ IPv4), bản ghi AAAA (địa chỉ IPv6), bản ghi CNAME (tên miền chuyển hướng), và nhiều loại khác.

Để thực hành nội dung này, sinh viên tạo thêm hai máy chủ mới chạy Window Server tên ALT2_WS2016_<MSSV> và ALT3_WS2016_<MSSV> sau đó thực hiện theo các bước hướng dẫn và đạt yêu cầu đầu ra theo *Tài liệu tham khảo 1* (từ trang 257 - 281). Đồng thời nội dung thực hành phải dựa trên bảng ánh xạ giá trị từ tài liệu tham khảo (bảng 1) và theo kiến trúc mạng được minh họa trên hình 2.

2. Cấu hình dịch vụ Backup DNS

Backup DNS trong Windows Server là một giải pháp dự phòng giúp đảm bảo tính sẵn sàng và độ tin cậy của dịch vụ DNS trong trường hợp máy chủ DNS chính gặp sự cố. Cơ chế này hoạt động bằng cách thiết lập một hoặc nhiều máy chủ DNS phụ (secondary DNS servers) để sao lưu dữ liệu từ máy chủ DNS chính (primary DNS server). Máy chủ DNS phụ thường xuyên cập nhật và đồng bộ hóa với máy chủ DNS chính thông qua một quá trình gọi là "zone transfer" (chuyển vùng). Trong quá trình này, các bản ghi DNS được sao chép từ máy chủ chính sang máy chủ phụ theo lịch trình định kỳ hoặc khi có thay đổi trong cơ sở dữ liệu vùng.

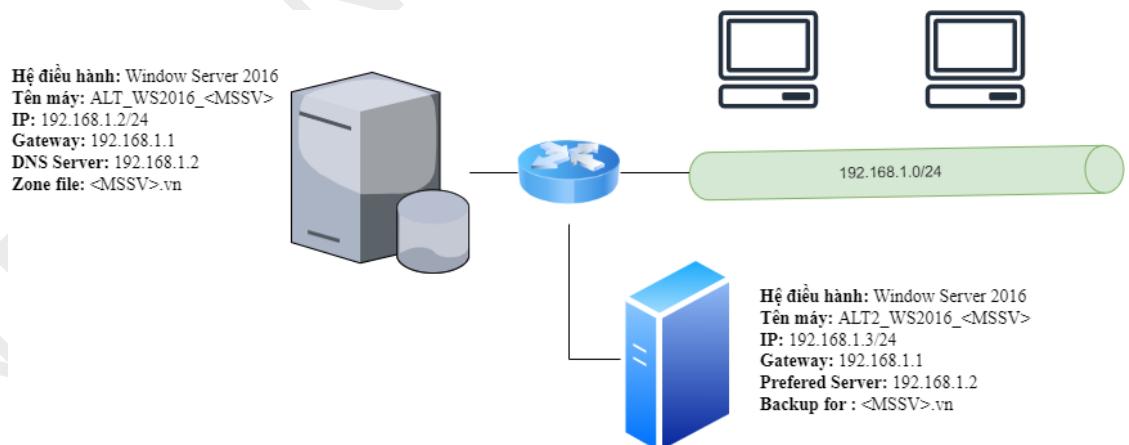
Backup DNS



CloudDNS

Hình 3: Minh họa cơ chế hoạt động của chức năng DNS Backup

Khi một máy khách gửi yêu cầu DNS, nếu máy chủ DNS chính không phản hồi hoặc không khả dụng, yêu cầu sẽ tự động được chuyển đến máy chủ DNS phụ. Điều này đảm bảo rằng dịch vụ phân giải tên miền không bị gián đoạn và các truy vấn DNS vẫn được xử lý một cách chính xác. Việc cấu hình backup DNS trong Windows Server không chỉ cung cấp một lớp bảo vệ bổ sung chống lại sự cố phần cứng hoặc phần mềm mà còn giúp cân bằng tải (load balancing) bằng cách phân phối các yêu cầu DNS giữa các máy chủ khác nhau. Điều này cải thiện hiệu suất tổng thể của mạng và đảm bảo dịch vụ DNS luôn hoạt động mượt mà và hiệu quả.



Hình 4: Kiến trúc mạng máy tính cho nội dung thực hành 2

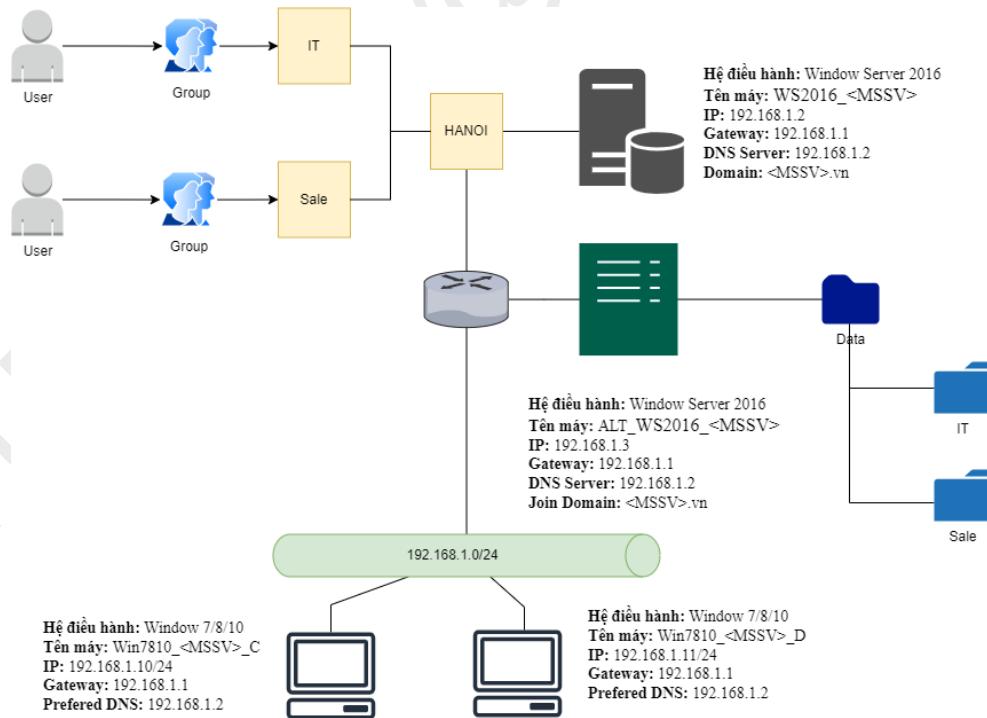
Để hoàn thành nội dung này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 1](#) trang 282 -309. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 4.

3. Cấu hình và phân quyền chia sẻ dữ liệu

Cấu hình và phân quyền chia sẻ dữ liệu trong Windows Server là quá trình thiết lập và quản lý việc chia sẻ các thư mục và tệp tin từ máy chủ để người dùng trong mạng có thể truy cập và sử dụng chúng. Để thực hiện điều này, người quản trị sẽ tạo các thư mục chia sẻ trên máy chủ, sau đó thiết lập quyền truy cập cho từng người dùng hoặc nhóm người dùng cụ thể. Quy trình này thường bắt đầu bằng việc sử dụng giao diện quản trị của Windows Server, như File and Storage Services hoặc File Explorer, để tạo thư mục chia sẻ mới. Khi tạo thư mục chia sẻ, người quản trị có thể cấu hình các quyền truy cập cơ bản như đọc, ghi và thực thi cho từng người dùng hoặc nhóm người dùng.

Để có sự linh hoạt và kiểm soát chi tiết hơn, người quản trị có thể sử dụng NTFS permissions để thiết lập quyền truy cập ở mức tệp và thư mục. NTFS permissions cho phép người quản trị kiểm soát cụ thể quyền của từng người dùng đối với từng tệp hoặc thư mục, bao gồm quyền đọc, ghi, thực thi, xóa và sở hữu.

Bằng cách cấu hình và phân quyền chia sẻ dữ liệu một cách chính xác, người quản trị đảm bảo rằng dữ liệu được bảo vệ và chỉ có những người dùng được ủy quyền mới có thể truy cập và thực hiện các hành động tương ứng với dữ liệu đó. Điều này đảm bảo tính an toàn và hiệu quả của việc chia sẻ dữ liệu trong môi trường mạng.



Hình 5: Kiến trúc mạng máy tính cho nội dung thực hành 3

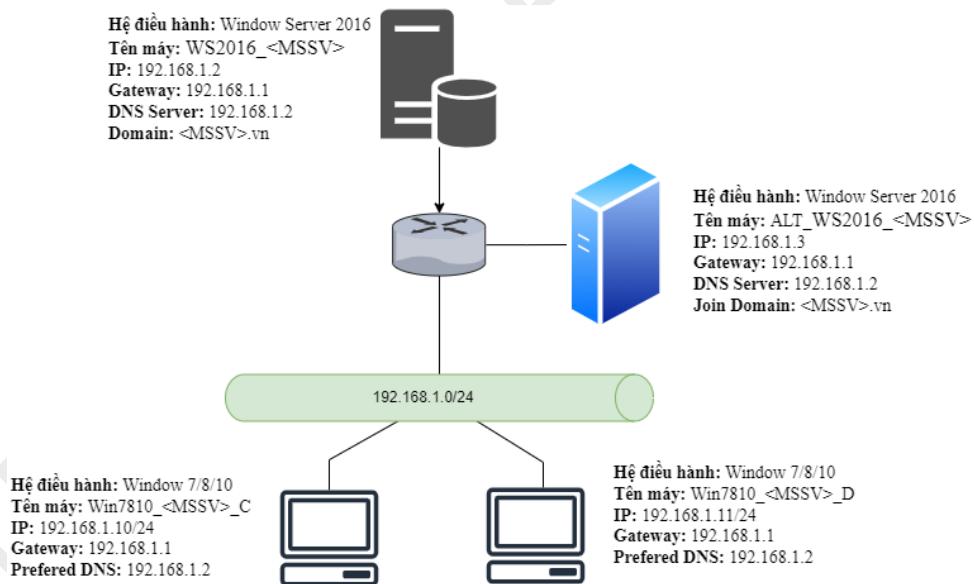
Để hoàn thành nội dung này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 1](#) trang 434 - 458. Lưu ý sinh viên cần tuân theo các giá trị sẽ

được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 5. SV có thể tham khảo lại cách tạo OU, Group và User trong bài LAB2.

4. Cấu hình Offline File

Cấu hình Offline Files trong Windows Server là quá trình cho phép người dùng lưu trữ và truy cập vào các tệp tin từ mạng mà không cần kết nối trực tiếp với máy chủ. Khi tính năng Offline Files được kích hoạt và cấu hình trên máy chủ, người dùng có thể đồng bộ hóa các tệp tin và thư mục từ máy chủ với máy tính cá nhân của họ. Điều này cho phép họ làm việc với tệp tin ngay cả khi không có kết nối mạng và tự động đồng bộ hóa thay đổi khi kết nối lại.

Để cấu hình Offline Files, người quản trị sẽ thiết lập chính sách nhóm (Group Policy) hoặc cấu hình trên máy chủ file để cho phép tính năng này. Sau đó, người dùng có thể chọn các thư mục hoặc tệp tin mà họ muốn lưu trữ offline trên máy tính cá nhân của mình. Khi họ kết nối với mạng, các thay đổi sẽ được đồng bộ hóa tự động giữa máy tính cá nhân và máy chủ.



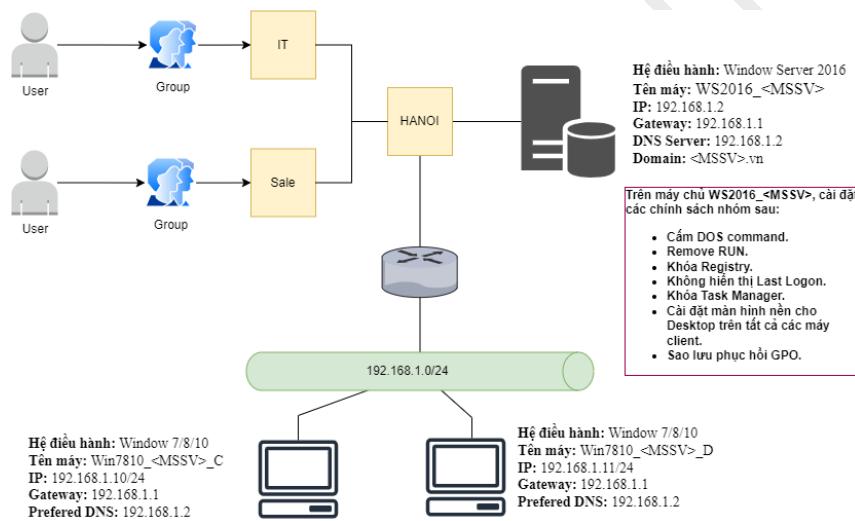
Hình 6: Kiến trúc mạng máy tính cho nội dung thực hành 4

Để hoàn thành nội dung này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 1](#) trang 507 - 535. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 6.

5. Triển khai chính sách GPO cơ bản

Chính sách nhóm (Group Policy) trong Windows Server là một cơ chế quản lý trung tâm cho phép người quản trị mạng thiết lập và áp dụng các cài đặt và hạn chế trên các máy tính và người dùng trong một mạng doanh nghiệp. Ý nghĩa của chính sách nhóm là tạo ra một môi trường mạng đồng nhất và an toàn, đồng thời giúp người quản trị quản lý và duy trì hệ thống một cách hiệu quả.

Ví dụ, người quản trị có thể sử dụng GPO để áp dụng các cài đặt bảo mật như đặt mật khẩu phức tạp, cấm việc sử dụng ổ đĩa USB, hoặc cấm truy cập vào các trang web không an toàn. Họ cũng có thể cấu hình các cài đặt hệ thống như đặt hình nền mặc định, thiết lập một môi trường làm việc nhất quán trên toàn hệ thống mạng.



Hình 7: Kiến trúc mạng máy tính cho nội dung thực hành 5

Để hoàn thành nội dung này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 1](#) trang 536 - 561. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 7.

6. Giám sát và bắt sự kiện thao tác với file trên máy chủ chính

Giám sát tệp tin và bắt sự kiện thao tác với file là một tính năng trong Windows Server giúp người quản trị mạng giám sát và kiểm soát các hoạt động (tạo mới, sửa, xóa, di chuyển...) liên quan đến tệp tin trên các máy tính trong mạng doanh nghiệp. Ý nghĩa của tính năng này là cung cấp một cách để theo dõi và bảo vệ dữ liệu quan trọng trước các hành động không mong muốn như xóa tệp tin quan trọng hoặc di chuyển chúng vào các vị trí không mong muốn. Ngoài ra, tính năng này cũng giúp

ngăn chặn các hành động độc hại như virus hoặc phần mềm độc hại thực hiện xóa hoặc sửa đổi dữ liệu trên hệ thống.

Ví dụ, một người quản trị có thể sử dụng tính năng giám sát tệp tin và bắt xóa file GPO để thiết lập chính sách giám sát trên các thư mục quan trọng như thư mục chia sẻ dữ liệu. Khi một tệp tin quan trọng bị xóa hoặc di chuyển, hệ thống sẽ ghi lại sự kiện này và cung cấp thông báo cho người quản trị, giúp họ nhanh chóng phát hiện và ứng phó với các vấn đề liên quan đến tệp tin. Điều này giúp tăng cường bảo mật và đảm bảo tính toàn vẹn của dữ liệu trong mạng.

Để hoàn thành nội dung này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 1](#) trang 562 - 580. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 5.

III. Quy định nộp bài thực hành

1. Sinh viên cần trình bày bài làm theo file template được GV cung cấp và nộp lại trên hệ thống LMS theo đúng deadline và các quy định liên quan.
2. Không chấp nhận những bài làm có dấu hiệu sao chép giống nhau và sẽ cho 0 điểm bài LAB của những bài làm này.

----HẾT----



I. Tóm tắt bài thực hành

1. Yêu cầu lý thuyết

Sinh viên đã được trang bị các kiến thức về phân quyền và chia sẻ dữ liệu trong WS2016 gồm:

- Triển khai dịch vụ Active Directory
- Triển khai Windows Deployment Services (WDS)
- Triển khai dịch vụ Internet Information Services (IIS)
- Triển khai cài đặt và cấu hình dịch vụ VPN Server

2. Nội dung chính bài thực hành

- Cài đặt và cấu hình Windows Deployment Services (WDS)
- Triển khai dịch vụ Internet Information Services (IIS)
- Triển khai cài đặt và cấu hình RODC (Read Only Domain Controller)
- Triển khai cấu hình dịch vụ VPN Server (Client to Site)
- Triển khai cài đặt và cấu hình dịch vụ VPN (Site to Site)
- Triển khai cài đặt và cấu hình dịch vụ VPN Server (Client to Site) –SSTP

Bảng 1: Bảng ánh xạ các giá trị liên quan

Gía trị trong tài liệu tham khảo 1	Gía trị ánh xạ tương ứng trong tài liệu thực hành	Ý nghĩa
BKAP-DC12-01	WS2016_<MSSV>	Tên máy chủ chính chạy WS2016
BKAP-SRV12-01	ALT_WS2016_<MSSV> ⇒ AWS_<MSSV>	Tên máy chủ phụ thứ nhất chạy WS2016
BKAP-SRV-12-02	ALT2_WS2016_<MSSV> ⇒ AWS2_<MSSV>	Tên máy chủ phụ thứ hai chạy WS2016
BKAP-SRV-12-03	ALT3_WS2016_<MSSV> ⇒ AWS3_<MSSV>	Tên máy chủ phụ thứ ba chạy WS2016
Bkaptech	<MSSV>	Tên Image Group
bkaptech.vn	<MSSV>.vn	Tên domain
bachkhoa-aptech.vn	<Ho_ten_SV>.vn	Tên miền website
bkap.vn	<Ten_SV>.vn	Tên miền website

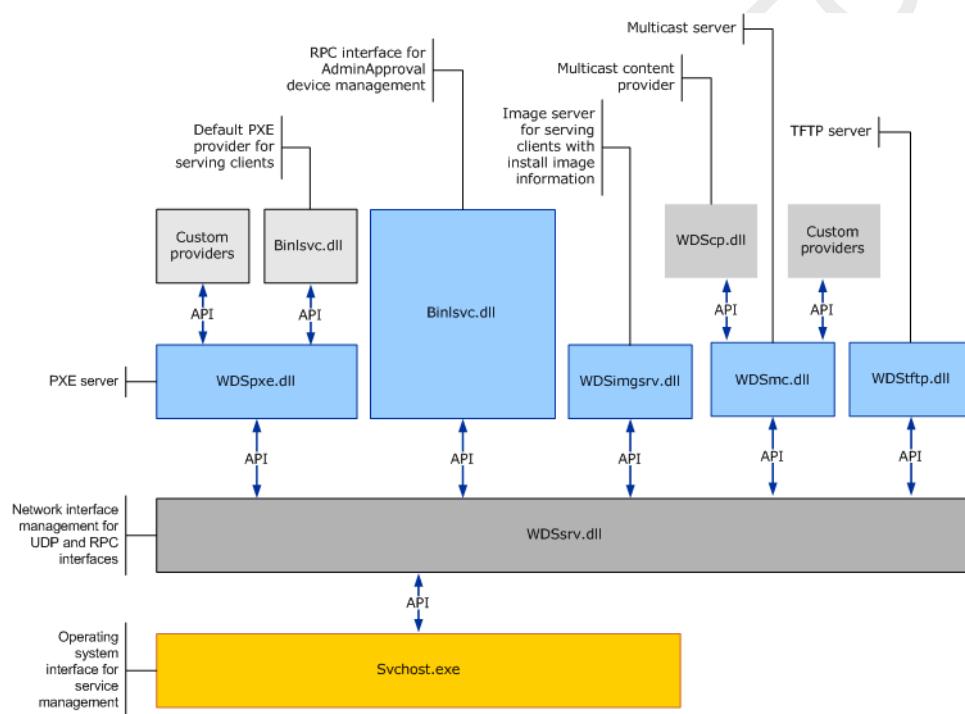
BKAP-WRK08-01	Win7810_<MSSV>_C	Tên máy client thứ nhất chạy Window 7/8/10
BKAP-WRK08-02	Win7810_<MSSV>_D	Tên máy client thứ hai chạy Window 7/8/10
duynh	<MSSV>us1 <ul style="list-style-type: none"> • First name: <MSSV> • Last name: us1 • Full name: <MSSV>us1 • User logon name: <MSSV>us1 (@<MSSV>.vn) • Password: 123456a@ 	
hungnq	<MSSV>us2 // Xử lý thông tin tài khoản user tương tự như trên.	
cuongvv	<MSSV>us3 // Xử lý thông tin tài khoản user tương tự như trên.	
quanch	<MSSV>us4 // Xử lý thông tin tài khoản user tương tự như trên	
truonglv	<MSSV>us5 // Xử lý thông tin tài khoản user tương tự như trên	
nghialv	<MSSV>us6 // Xử lý thông tin tài khoản user tương tự như trên	

II. Chi tiết bài thực hành

1. Cài đặt và cấu hình WDS

Windows Deployment Services (WDS) trong Windows Server là một dịch vụ cho phép triển khai hệ điều hành Windows qua mạng mà không cần phải cài đặt thủ công

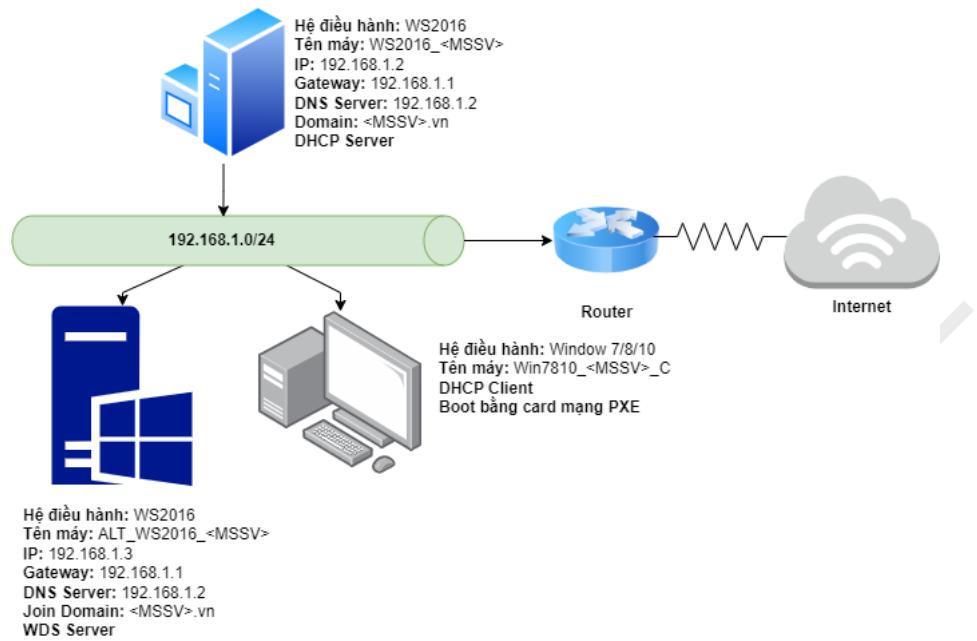
từ các phương tiện vật lý như DVD hoặc USB trên từng máy client. WDS hoạt động bằng cách sử dụng các giao thức PXE (Preboot Execution Environment) và TFTP (Trivial File Transfer Protocol) để khởi động và truyền dữ liệu từ một máy chủ tới các máy khách trên mạng. Khi một máy khách khởi động, nó sẽ gửi yêu cầu PXE tới mạng và nhận được một tệp khởi động (boot image) từ máy chủ WDS. Sau đó, máy khách sẽ sử dụng tệp khởi động này để tải hệ điều hành từ máy chủ và tiến hành cài đặt tự động. WDS giúp quản trị viên hệ thống tiết kiệm thời gian và công sức trong việc triển khai hàng loạt hệ điều hành, đồng thời cung cấp các tính năng như cài đặt không cần giám sát và triển khai hình ảnh (imaging) tùy chỉnh.



Hình 1: Sơ đồ các thành phần trong dịch vụ WDS

Ví dụ theo hình 1, giả sử một công ty cần triển khai hệ điều hành Windows 8 cho 100 máy tính mới. Thay vì cài đặt hệ điều hành thủ công trên từng máy, quản trị viên hệ thống sử dụng WDS để tự động hóa quá trình này. Đầu tiên, quản trị viên sẽ cài đặt và cấu hình WDS trên một máy chủ Windows Server. Tiếp theo, họ tạo và tải lên một tệp khởi động (boot image) và một tệp cài đặt (install image) của Windows 10 lên máy chủ WDS. Các tệp này chứa mọi thứ cần thiết để khởi động và cài đặt hệ điều hành. Khi máy tính mới được bật, chúng sẽ tự động gửi yêu cầu PXE tới mạng để tìm máy chủ WDS. Máy chủ WDS sẽ phản hồi và cung cấp tệp khởi động qua TFTP. Máy tính sẽ sử dụng tệp khởi động này để khởi động vào môi trường cài đặt Windows. Sau đó,

tệp cài đặt Windows 10 sẽ được truyền từ máy chủ WDS tới máy tính khách và quá trình cài đặt tự động sẽ bắt đầu.



Hình 2: Minh họa kiến trúc hệ thống mạng cho nội dung thực hành 1

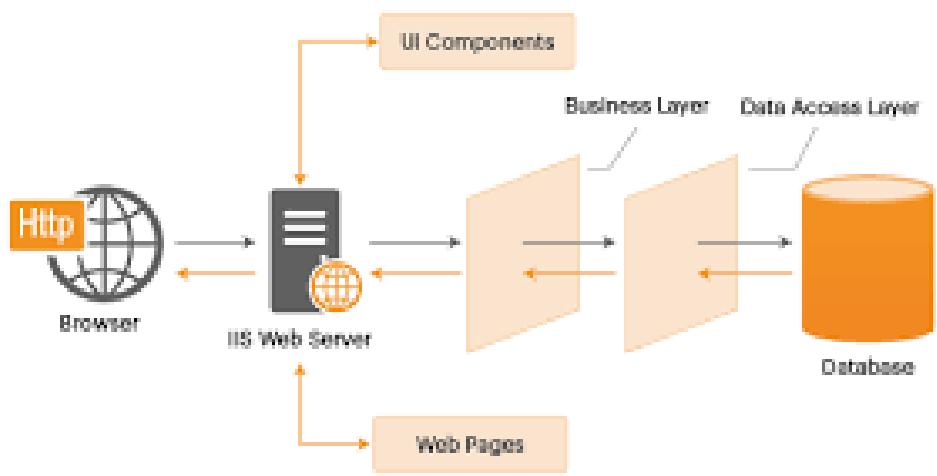
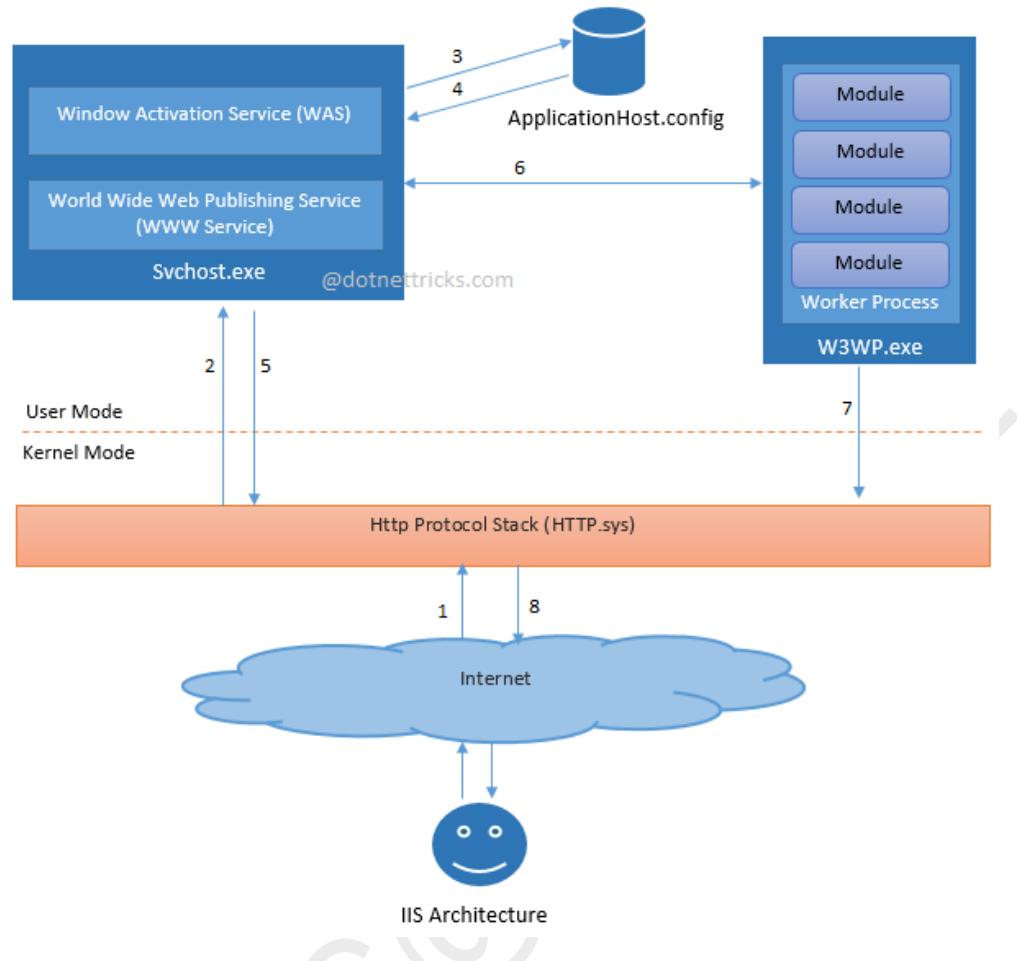
Để hoàn thành nội dung này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 3](#) trang 4 - 29. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 2. *Lưu ý, nếu máy client Win7810_<MSSV>_C của SV đã cài đặt sẵn hệ điều hành thì có thể tạo một máy client mới chưa cài hệ điều hành nào đặt tên là Win8_<MSSV>_E. Ngoài ra, SV có thể vào hệ thống LMS để lấy link file iso cài đặt hệ điều hành Win 8.*

2. Triển khai dịch vụ IIS

IIS (Internet Information Services) là một **máy chủ web** (web server) do Microsoft phát triển, dùng để **lưu trữ, quản lý và cung cấp các trang web, ứng dụng web và dịch vụ web**. IIS hỗ trợ nhiều giao thức như **HTTP, HTTPS, FTP, FTPS, SMTP...**

Ngoài ra, IIS còn có các tính năng sau:

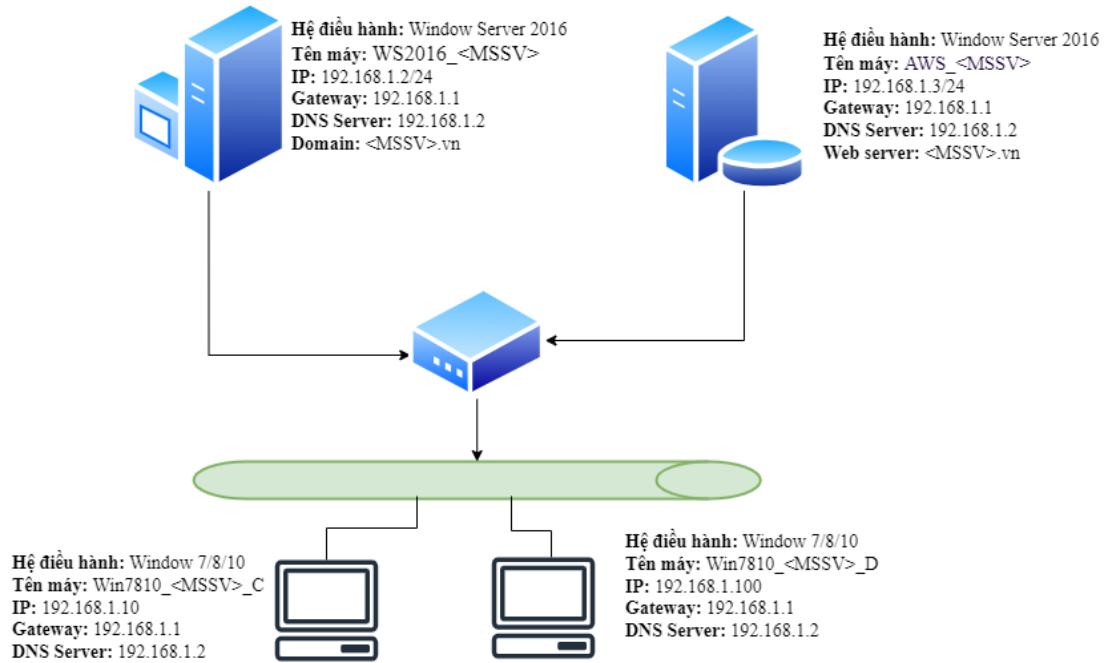
- Chạy trang web và ứng dụng web (ASP.NET, PHP, Node.js, v.v.).
- Quản lý yêu cầu HTTP/HTTPS và xử lý chúng thông qua Worker Process (w3wp.exe).
- Hỗ trợ cân bằng tải và bảo mật (SSL/TLS, xác thực Windows, lọc yêu cầu, v.v.).
- Triển khai dịch vụ Web API, WebSocket, và các ứng dụng microservices.



Hình 3: Kiến trúc dịch vụ IIS

Trong phần này, SV sẽ thực thi các nội dung sau:

2.1. Cấu hình IIS với Single Website



Hình 4: Minh họa kiến trúc hệ thống mạng cho nội dung thực hành 2.1 và 2.2

Để hoàn thành nội dung này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 3](#) trang 31 - 39. Lưu ý:

- SV cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 4.
- Đổi tên thư mục Website BachkhoaAptech thành Website_MSSV**

2.2. Cấu hình Multi Website kết hợp với DNS Server

Để hoàn thành nội dung này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 3](#) trang 39 - 49. Lưu ý:

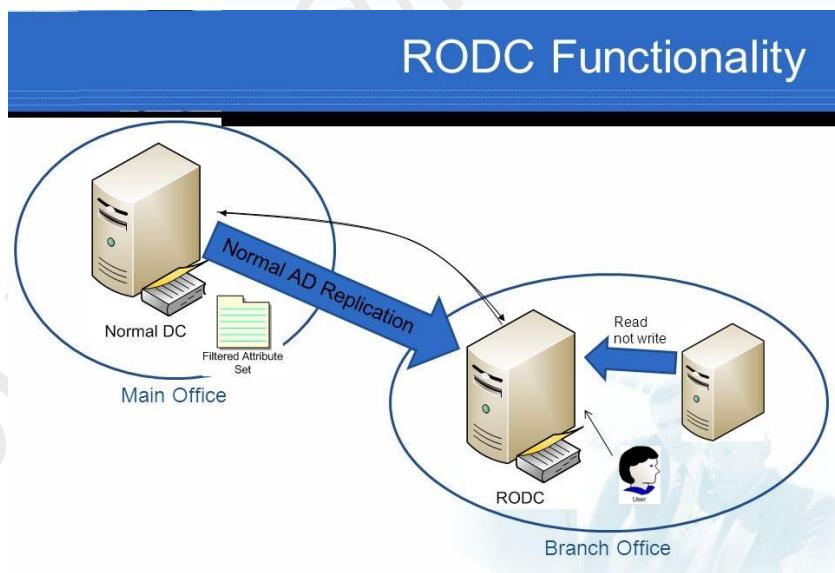
- SV cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 4.
- Đổi tên miền website theo quy tắc như trong bảng 1. Ví dụ:**
 - www.bkaptech.vn → www.635017xxx.vn
 - www.bachkhoa-aptech.vn → www.nguyenthienthieu.com.vn
 - www.bkap.vn → www.duong.vn

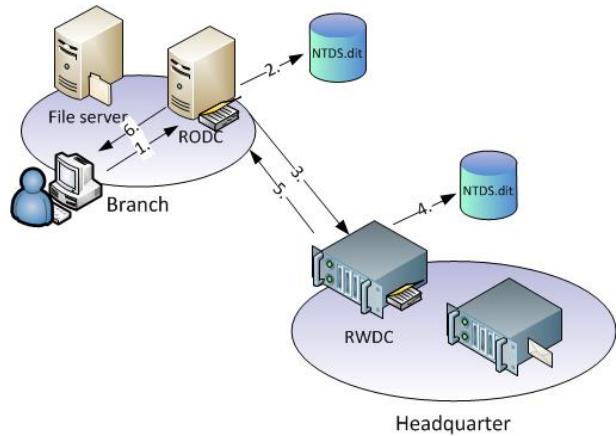
3. Cài đặt và cấu hình RODC

RODC (Read-Only Domain Controller) là một loại Domain Controller trong cơ sở dữ liệu Active Directory của Microsoft. Khác với các domain controller thông thường,

RODC chỉ cho phép truy cập dữ liệu chỉ đọc từ Active Directory, không thực hiện các thay đổi trực tiếp vào cơ sở dữ liệu.

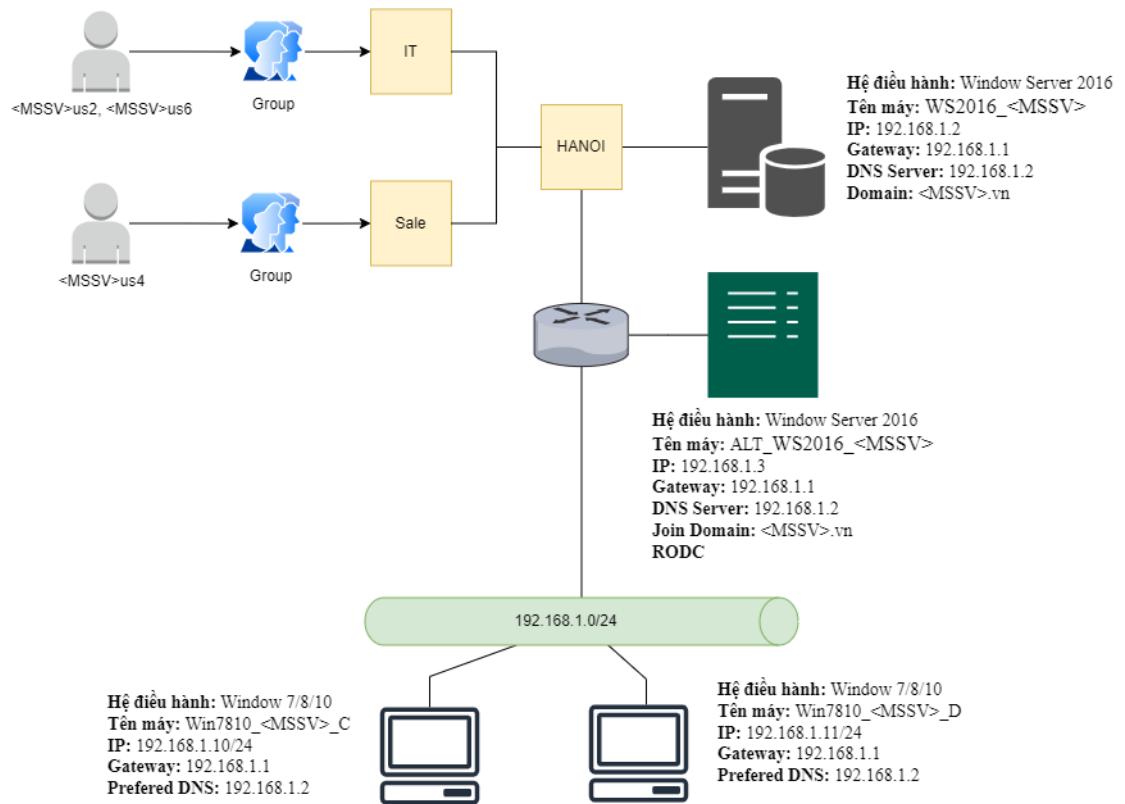
Hoạt động của RODC là cung cấp dịch vụ xác thực và truy cập cho người dùng và các thiết bị trong mạng, đặc biệt là trong các môi trường mạng như các chi nhánh văn phòng hoặc các môi trường không đảm bảo về bảo mật. RODC hoạt động với NTDS (NT Directory Services - là một tập hợp các dịch vụ và thành phần phần mềm được sử dụng để lưu trữ và quản lý thông tin về tài nguyên mạng, người dùng, nhóm và các đối tượng khác trong một mạng Windows). Khi một người dùng cố gắng truy cập vào tài nguyên trong mạng, RODC sẽ tìm kiếm thông tin xác thực từ NTDS. Tuy nhiên, do tính chất chỉ đọc, RODC sẽ gửi yêu cầu này đến một DC khác, gọi là "Read-Write Domain Controller" (RWDC), nơi dữ liệu có thể được thay đổi. RWDC sẽ xác minh thông tin xác thực và trả về cho RODC, sau đó RODC sẽ chuyển tiếp thông tin này cho người dùng. Khi RODC nhận được thông tin từ RWDC, nó sẽ lưu trữ một bản sao của dữ liệu này trong bộ nhớ cache để tăng hiệu suất cho các yêu cầu sau này và giảm bớt tải cho RWDC. Qua đó, RODC giúp cải thiện bảo mật và hiệu suất cho mạng Windows Server.





Hình 5: Cách thức hoạt động

Ví dụ, hãy tưởng tượng bạn là quản trị viên mạng của một công ty có nhiều chi nhánh văn phòng. Mỗi chi nhánh có một số lượng người dùng và thiết bị đủ lớn để cần một domain controller địa phương để quản lý các tài khoản người dùng, quyền truy cập, và các tài nguyên mạng. Khi đó, bạn quyết định triển khai một RODC tại mỗi chi nhánh văn phòng. Khi một nhân viên tại một chi nhánh cố gắng truy cập vào tài nguyên được lưu trữ hoặc có kết nối đến mạng máy chủ của cả công ty (chẳng hạn như máy in hoặc thư mục chia sẻ) RODC sẽ xác thực người dùng và cung cấp quyền truy cập tương ứng. Điều quan trọng là RODC không lưu trữ tất cả dữ liệu của Active Directory, mà chỉ sao chép một phần dữ liệu từ domain controller chính. Vì vậy, nếu RODC tại một chi nhánh văn phòng bị tấn công và bị chiếm quyền, thông tin chỉ là một bản sao không thể sửa đổi của dữ liệu chính, giúp bảo vệ Active Directory của toàn bộ mạng. Trong khi đó, tại trung tâm dữ liệu chính hoặc các văn phòng chính, bạn có thể triển khai các domain controller chính (writable domain controller) để thực hiện các thay đổi vào Active Directory và đồng bộ hóa dữ liệu với các RODC ở các chi nhánh văn phòng.



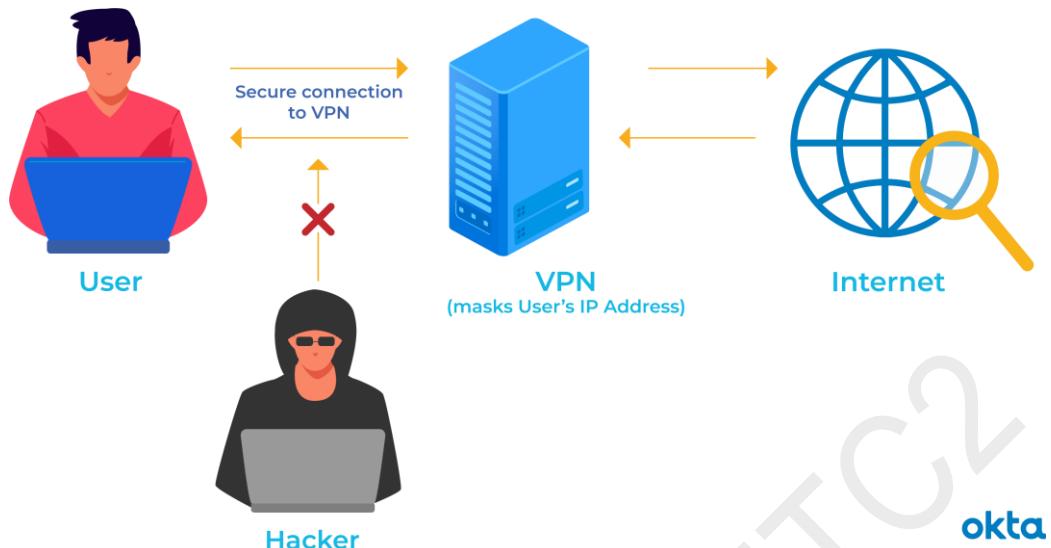
Hình 6: Minh họa kiến trúc hệ thống mạng cho nội dung thực hành 3

Để hoàn thành nội dung này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 3](#) trang 77 - 106. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 6

4. Triển khai cấu hình dịch vụ VPN Server (Client to Site)

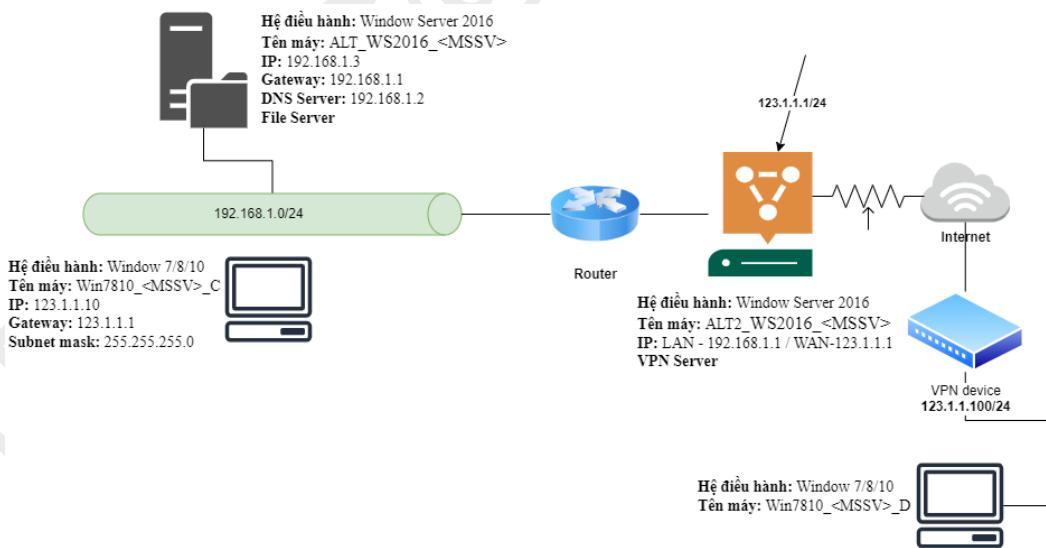
Dịch vụ VPN Server (Client to Site) trên Windows Server là một phần mềm hoặc tính năng được cài đặt trên máy chủ chạy hệ điều hành Windows Server để cung cấp khả năng kết nối an toàn cho các máy tính cá nhân hoặc thiết bị di động từ xa đến mạng nội bộ của tổ chức thông qua internet. VPN (Virtual Private Network) cho phép người dùng truy cập vào các tài nguyên mạng như tệp tin, máy chủ, và ứng dụng từ xa một cách bảo mật và riêng tư.

Khi được cấu hình và kích hoạt, VPN Server trên Windows Server sẽ tạo ra một kênh kết nối an toàn và mã hóa giữa máy tính cá nhân của người dùng và mạng nội bộ của tổ chức. Khi người dùng kết nối vào VPN từ xa, dữ liệu của họ sẽ được mã hóa và gửi qua kênh VPN trước khi đến máy chủ. Máy chủ sẽ giải mã dữ liệu và đưa vào mạng nội bộ, cho phép người dùng truy cập vào các tài nguyên mạng như khi họ ở trong văn phòng.



Hình 7: Minh họa cách hoạt động của tính năng VPN theo mô hình Client to Site

Để hoàn thành nội dung này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 3](#) trang 207 - 234. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 8. **Lưu ý, SV cần đổi tên thư mục Data thành Data_<MSV>.**

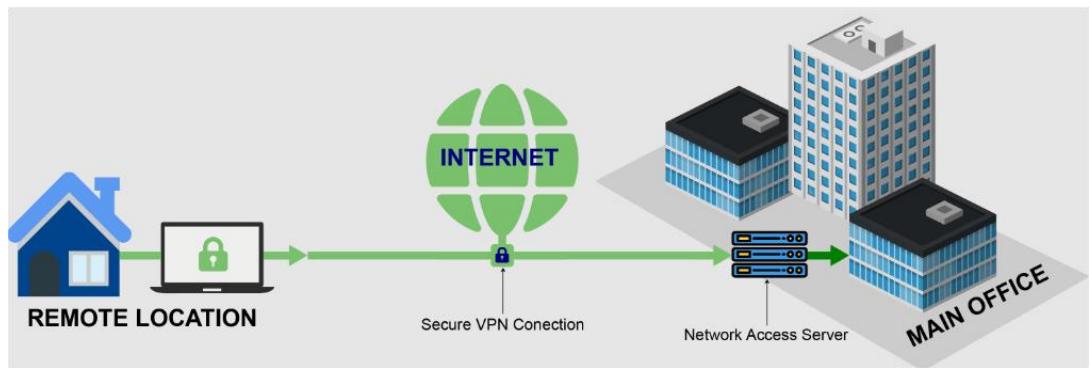


Hình 8: Minh họa kiến trúc hệ thống mạng cho nội dung thực hành 4

5. Triển khai cài đặt và cấu hình dịch vụ VPN (Site to Site)

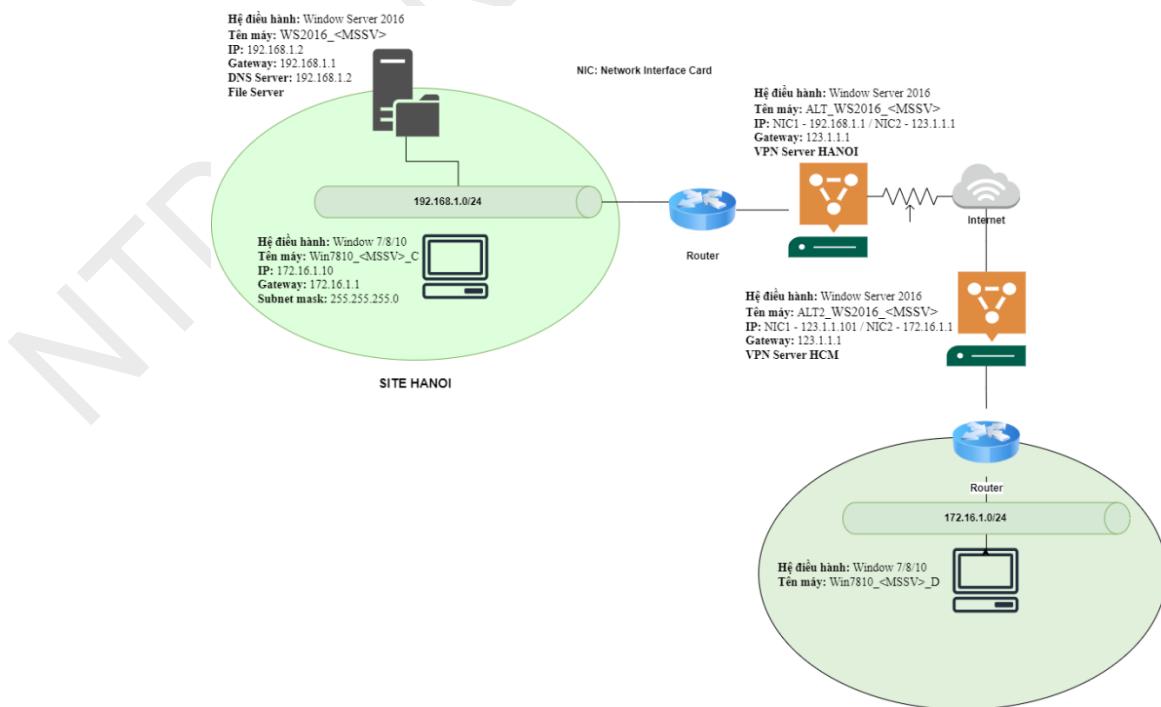
Tính năng VPN theo kiểu Site-to-Site là một tính năng khác của VPN được sử dụng để kết nối hai mạng LAN (Local Area Network) khác nhau thông qua internet. Trong kiểu này, không phải là các máy tính cá nhân hoặc thiết bị di động kết nối đến mạng

VPN mà là các mạng LAN của các tổ chức hoặc văn phòng được kết nối với nhau. Khi sử dụng tính năng này, các thiết bị mạng như router hoặc firewall ở mỗi văn phòng hoặc chi nhánh sẽ được cấu hình để tạo ra kết nối VPN trực tiếp với nhau. Khi kết nối được thiết lập, các dữ liệu giữa hai văn phòng sẽ được mã hóa và truyền qua kênh VPN an toàn, cho phép các máy tính và thiết bị trong mạng nội bộ của mỗi văn phòng truy cập vào tài nguyên của nhau như máy chủ, máy in, hoặc các thiết bị mạng khác.



Hình 9: Minh họa cách hoạt động của tính năng VPN theo mô hình Site to Site

Ví dụ, một công ty có hai chi nhánh ở hai địa điểm khác nhau. Mỗi chi nhánh có một mạng LAN riêng và một router hoặc firewall. Các router hoặc firewall ở mỗi chi nhánh được cấu hình để tạo ra một kết nối VPN site-to-site với nhau thông qua internet. Khi kết nối được thiết lập, các nhân viên ở mỗi chi nhánh có thể truy cập vào tài nguyên mạng của nhau một cách an toàn và riêng tư, giống như họ đang kết nối vào mạng LAN trong văn phòng của mình.



Hình 10: Minh họa kiến trúc hệ thống mạng cho nội dung thực hành 5

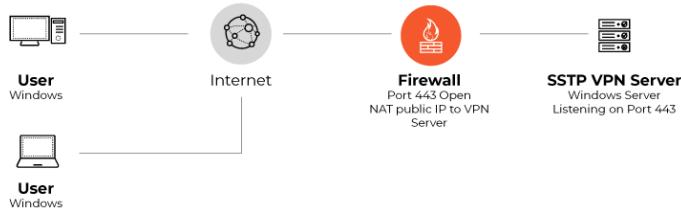
Để hoàn thành nội dung này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 3](#) trang 234 - 276. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 10. *Lưu ý, SV cần đổi tên thư mục Data thành Data_<MSV>.*

6. Cài đặt và cấu hình VPN (client to site) – SSTP

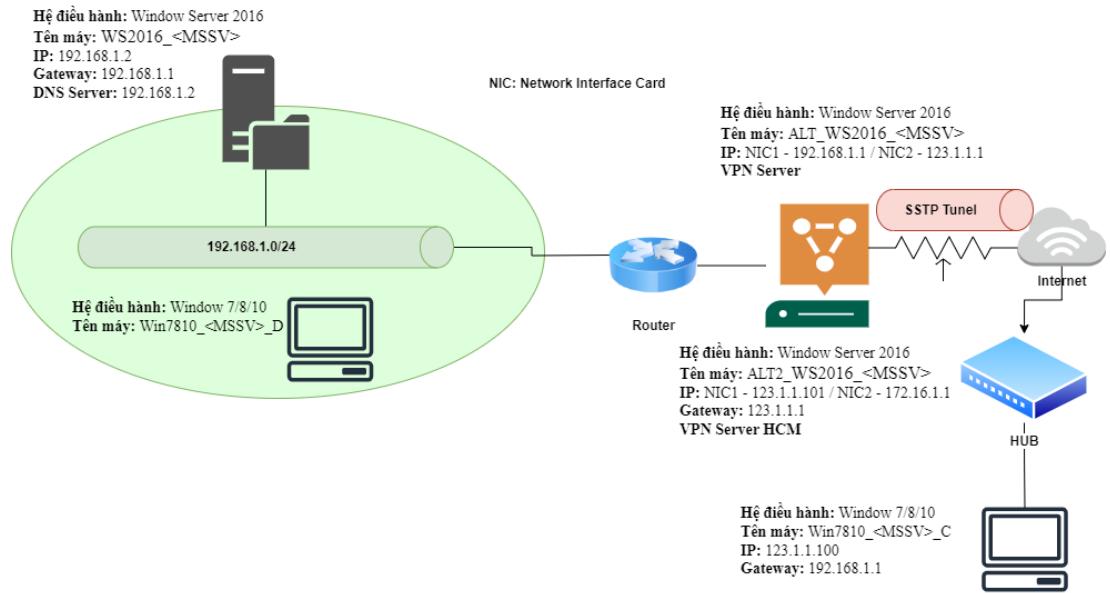
VPN Server (Client to Site) – SSTP NAT là một tính năng của dịch vụ VPN trên Windows Server, trong đó SSTP (Secure Socket Tunneling Protocol) được sử dụng để thiết lập kết nối VPN an toàn giữa máy tính cá nhân của người dùng và máy chủ VPN trên Windows Server thông qua internet. NAT (Network Address Translation) là một công nghệ thường được sử dụng để chuyển đổi các địa chỉ IP và cổng của gói tin mạng khi chúng đi qua một thiết bị mạng như router hoặc firewall.

Khi kết hợp với SSTP, tính năng NAT trên VPN Server (Client to Site) cho phép các gói tin VPN đi qua một máy chủ NAT trên đường truyền internet mà không làm mất tính bảo mật của kết nối VPN. Cụ thể, khi gói tin VPN đi qua máy chủ NAT, địa chỉ IP nguồn và đích trong gói tin được thay đổi để phù hợp với cấu hình mạng của mạng internet công cộng, nhưng dữ liệu bên trong vẫn được giữ nguyên và an toàn.

SSTP VPN Configuration



Hoạt động của SSTP NAT làm cho việc triển khai kết nối VPN trở nên linh hoạt và dễ dàng hơn trong các môi trường mạng phức tạp, nơi mà NAT được sử dụng để quản lý địa chỉ IP và bảo vệ mạng khỏi các mối đe dọa từ internet. Điều này giúp cho việc sử dụng VPN trở nên hiệu quả và bảo mật hơn trong các tổ chức và doanh nghiệp.



Hình 11: Minh họa kiến trúc hệ thống mạng cho nội dung thực hành 6

Để hoàn thành nội dung này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 3](#) trang 276 - 338. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 11.

III. Quy định nộp bài thực hành

- Sinh viên cần trình bày bài làm theo file template được GV cung cấp và nộp lại trên hệ thống LMS theo đúng deadline và các quy định liên quan.
- Không chấp nhận những bài làm có dấu hiệu sao chép giống nhau và sẽ cho 0 điểm bài LAB của những bài làm này.

----HẾT----



I. Tóm tắt bài thực hành

1. Yêu cầu lý thuyết

Sinh viên đã được trang bị các kiến thức về phân quyền và chia sẻ dữ liệu trong WS2016 gồm:

- Triển khai dịch vụ File Service.
- Triển khai dịch vụ Network Load Balancer.
- Triển khai dịch vụ Failover Clustering.

2. Nội dung chính bài thực hành

- Cấu hình Quota, File Screening và Tạo thông kê lưu trữ.
- Triển khai cài đặt và cấu hình dịch vụ DFS (Distributed File System).
- Đồng bộ dữ liệu trên 2 Server sử dụng DFS Replication.
- Triển khai Network Load Balancing.
- Cấu hình Failover Clustering.
- Sao lưu và phục hồi dữ liệu sử dụng Windows Server Backup.

Bảng 1: Bảng ánh xạ các giá trị liên quan

Gía trị trong tài liệu tham khảo 1	Gía trị ánh xạ tương ứng trong tài liệu thực hành	Ý nghĩa
BKAP-DC12-01	WS2016_<MSV>	Tên máy chủ chính chạy WS2016
BKAP-SRV12-01	ALT_WS2016_<MSV>	Tên máy chủ phụ thứ nhất chạy WS2016
BKAP-SRV-12-02	ALT2_WS2016_<MSV>	Tên máy chủ phụ thứ hai chạy WS2016
BKAP-SRV-12-03	ALT3_WS2016_<MSV>	Tên máy chủ phụ thứ ba chạy WS2016
Bkaptech	<MSV>	Tên Image Group
bkaptech.vn.	<MSV>.vn	Tên domain
BKAP-WRK08-01	Win7810_<MSV>_C	Tên máy client thứ nhất chạy Window 7/8/10
BKAP-WRK08-02	Win7810_<MSV>_D	Tên máy client thứ hai chạy Window 7/8/10

duynh	<p><MSSV>us1</p> <ul style="list-style-type: none"> • First name: <MSSV> • Last name: us1 • Full name: <MSSV>us1 • User logon name: <MSSV>us1 (@<MSSV>.vn) • Password: 123456a@ 	
hungnq	<p><MSSV>us2</p> <p>// Xử lý thông tin tài khoản user tương tự như trên.</p>	
cuongvv	<p><MSSV>us3</p> <p>// Xử lý thông tin tài khoản user tương tự như trên.</p>	
quanch	<p><MSSV>us4</p> <p>// Xử lý thông tin tài khoản user tương tự như trên</p>	
truonglv	<p><MSSV>us5</p> <p>// Xử lý thông tin tài khoản user tương tự như trên</p>	
nghialv	<p><MSSV>us6</p> <p>// Xử lý thông tin tài khoản user tương tự như trên</p>	

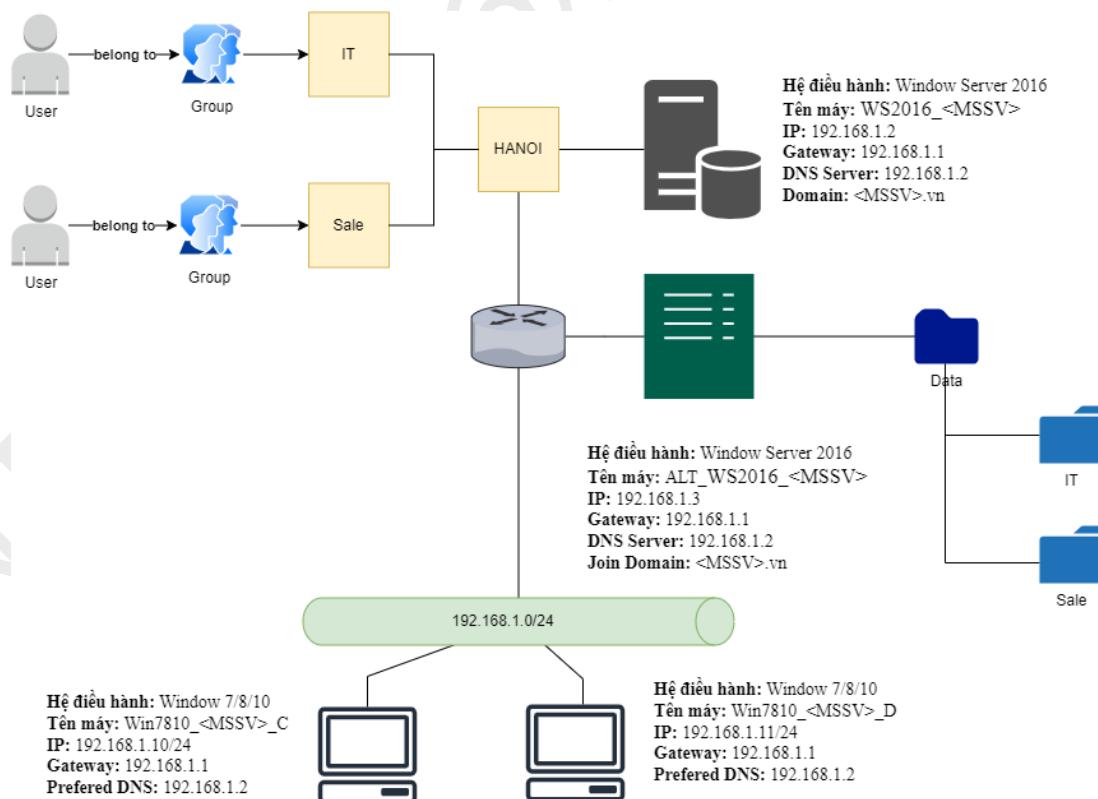
II. Chi tiết bài thực hành

1. Cấu hình Quota, File Screening và tạo thông kê lưu trữ

FSRM (File Server Resource Manager) trong Windows Server là một công cụ quản lý mạnh mẽ được sử dụng để quản lý và kiểm soát dữ liệu trên các máy chủ file. FSRM hoạt động bằng cách theo dõi và quản lý hoạt động file trên máy chủ, áp dụng các chính sách đã định nghĩa sẵn để duy trì việc sử dụng tài nguyên một cách hiệu quả và có tổ chức. Công cụ này giúp các quản trị viên hệ thống đảm bảo rằng dữ liệu được

lưu trữ hợp lý, ngăn ngừa việc sử dụng không kiểm soát và cải thiện tổng thể hiệu quả quản lý lưu trữ. Các tính năng chính của FSRM bao gồm:

- Quản lý hạn ngạch (Quota Management): Cho phép quản trị viên thiết lập và quản lý các hạn ngạch lưu trữ trên các thư mục hoặc ổ đĩa cụ thể, giúp kiểm soát và ngăn chặn việc sử dụng quá mức dung lượng lưu trữ trên máy chủ tệp.
- Quản lý tập tin (File Management Tasks): Cung cấp các công cụ để tự động thực hiện các nhiệm vụ quản lý tệp như di chuyển, sao chép hoặc xóa tệp dựa trên các quy tắc và chính sách được thiết lập bởi quản trị viên.
- Sàng lọc file (File Screening): Cho phép quản trị viên áp dụng các chính sách sàng lọc tệp để ngăn chặn việc lưu trữ các loại tệp không mong muốn hoặc nguy hiểm trên máy chủ tệp, ví dụ có thể sàng lọc tệp theo phần mở rộng, kích thước hoặc nội dung, ...
- Báo cáo lưu trữ (Storage Reports): Tạo ra các báo cáo chi tiết về việc sử dụng dung lượng lưu trữ trên máy chủ tệp. Bao gồm thông tin về dung lượng sử dụng, loại tệp, xu hướng sử dụng và các chỉ số khác giúp quản trị viên đánh giá hiệu suất và tối ưu hóa tài nguyên lưu trữ.



Hình 1: Minh họa kiến trúc hệ thống mạng cho nội dung thực hành 1 và 2

- Hạ tầng phân loại tệp (File Classification Infrastructure): Cung cấp cơ sở hạ tầng cho việc phân loại tệp dựa trên các thuộc tính như loại tệp, độ nhạy cảm, hoặc giá trị kinh doanh, giúp tự động phân loại và gắn nhãn cho các tệp dựa trên các quy tắc và chính sách được thiết lập.

Để hoàn thành nội dung thực hành này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 3](#) trang 540 - 565. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 1.

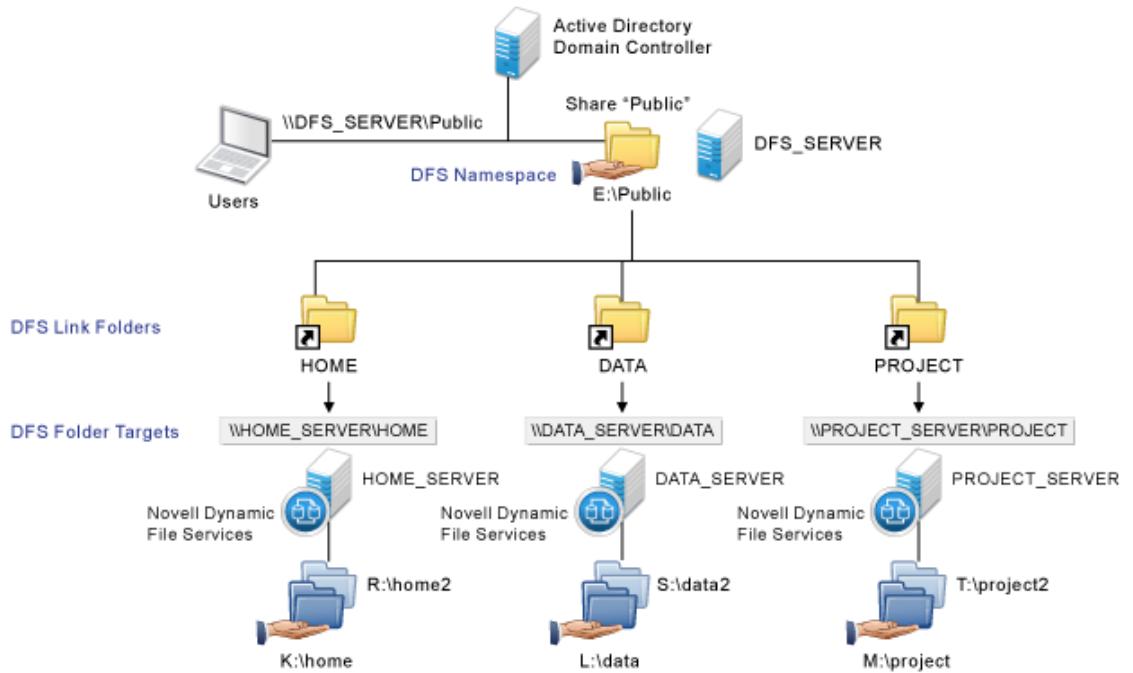
2. Triển khai cài đặt và cấu hình dịch vụ DFS (Distributed File System)

Distributed File System (DFS) trong Windows Server là một dịch vụ giúp tổ chức và quản lý tập tin trên mạng máy tính một cách hiệu quả bằng cách tạo ra một không gian tên (namespace) tập tin phân tán, tức là một không gian tập tin ảo gồm các tài nguyên từ nhiều máy chủ khác nhau, thay vì tập trung các tập tin này vào một máy chủ duy nhất. Các thành phần chính của DFS bao gồm DFS Server, DFS Namespace, DFS Link Folder và DFS Folder Target (hình 2). Cụ thể:

- DFS Server: Là máy chủ cung cấp dịch vụ DFS, nơi chứa tài nguyên tập tin được chia sẻ trên mạng.
- DFS Namespace: Là một không gian tên ảo mà người dùng truy cập để đến các tập tin và thư mục trên mạng được chia sẻ chung, giúp che giấu sự phân tán của tài nguyên và tạo ra sự nhất quán cho người dùng khi truy cập tập tin từ nhiều máy chủ.
- DFS Link Folder: Là các thư mục được tạo ra trong DFS Namespace để đại diện cho tài nguyên thực sự nằm trên các máy chủ khác nhau.
- DFS Folder Target: Là các đường dẫn thực tế đến tài nguyên tập tin trên các máy chủ. Mỗi DFS Link Folder sẽ có ít nhất một DFS Folder Target, nhưng có thể có nhiều hơn một để cung cấp tính sẵn sàng và dự phòng.

Ví dụ một công ty lớn có nhiều chi nhánh trên khắp đất nước, mỗi chi nhánh có các máy chủ riêng chứa các tập tin và dữ liệu quan trọng. Để quản lý tập tin một cách hiệu quả và cung cấp trải nghiệm nhất quán cho nhân viên, công ty đã triển khai DFS (Distributed File System). Khi một nhân viên tại chi nhánh A muốn truy cập vào tài liệu quan trọng nằm trên máy chủ của chi nhánh B, thay vì phải biết chính xác địa chỉ máy chủ của chi nhánh B, người này chỉ cần truy cập vào DFS Namespace của công ty. DFS Namespace tạo ra một không gian tên ảo, trong đó tất cả các tài nguyên tập tin

được tổ chức một cách logic và áô tính chia sẻ chung. Nhân viên có thể điều hướng đến thư mục "Tài liệu Quan Trọng" trong DFS Namespace và tìm thấy một liên kết thư mục (DFS Link Folder) được đặt tên là "Chi Nhánh B". Khi anh ta mở liên kết này, DFS sẽ tự động định tuyến anh ta đến máy chủ của chi nhánh B, nơi chứa thư mục "Tài liệu Quan Trọng".



Hình 2: Kiến trúc chung của dịch vụ DFS

Nhờ vào DFS, người dùng không cần biết về cấu trúc phân tán của tập tin hay địa chỉ cụ thể của các máy chủ, mà vẫn có thể truy cập tập tin một cách dễ dàng và nhất quán. Đồng thời, DFS cũng cho phép quản trị viên dễ dàng thêm, xóa hoặc di chuyển các tài nguyên mà không làm ảnh hưởng đến trải nghiệm người dùng.

Để hoàn thành nội dung thực hành này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 3](#) trang 565 - 581. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 1.

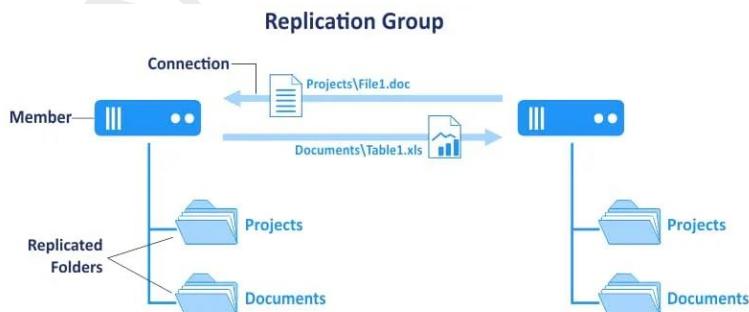
3. Đồng bộ dữ liệu trên 2 Server sử dụng DFS Replication

Một số tính năng nổi bật trong DFS có thể kể đến như:

- File Replication: Sao chép tệp tin giữa các máy chủ để tăng tính sẵn có và độ tin cậy.
- File Sharing: Chia sẻ tệp tin giữa các máy tính trong mạng một cách dễ dàng và hiệu quả.

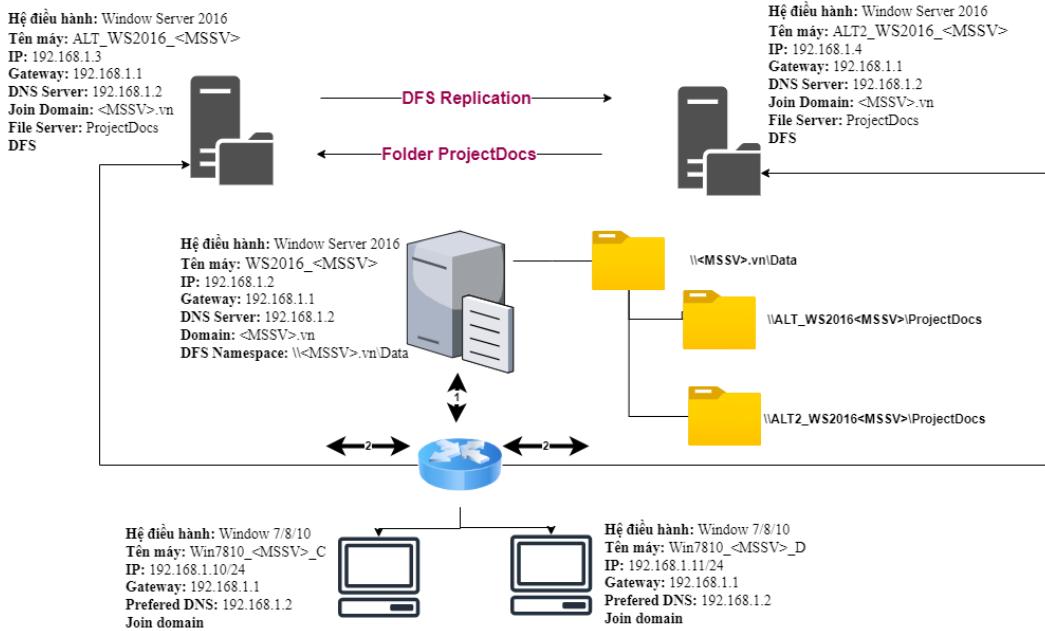
- Scalability: Khả năng mở rộng của hệ thống để phục vụ cho một lượng lớn người dùng và tải công việc.
- Fault Tolerance: Tính khả năng chịu lỗi, đảm bảo rằng hệ thống vẫn hoạt động một cách đáng tin cậy ngay cả khi có sự cố xảy ra.
- Load Balancing: Phân phối tải công việc đều đặn giữa các máy chủ để tối ưu hóa hiệu suất hệ thống.

Một trong những tính năng nổi bật nhất của DFS là Replication là một cơ chế quan trọng giúp tăng tính sẵn có và độ tin cậy của dữ liệu. Khi một tệp tin được tạo mới hoặc sửa đổi trên máy chủ nguồn, hệ thống DFS sẽ tự động sao chép tệp tin này sang một hoặc nhiều máy chủ đích khác. Quá trình sao chép này có thể được cấu hình để diễn ra tự động hoặc theo lịch trình nhất định. Một khi tệp tin được sao chép sang các máy chủ đích, người dùng có thể truy cập và sử dụng chúng từ bất kỳ máy chủ nào trong hệ thống DFS mà họ có quyền truy cập. Điều này tạo ra một môi trường làm việc linh hoạt và đồng nhất, nơi dữ liệu luôn sẵn sàng và có thể được truy cập từ nhiều điểm trên mạng. Tính năng sao chép tệp tin không chỉ tăng tính sẵn có và độ tin cậy của dữ liệu mà còn cung cấp khả năng chống lại sự cố hardware hoặc phần mềm trên một máy chủ cụ thể. Nếu một máy chủ gặp sự cố, người dùng vẫn có thể truy cập dữ liệu từ các bản sao trên các máy chủ khác trong hệ thống DFS. Điều này giúp giảm thiểu thời gian chết và giữ cho dịch vụ hoạt động một cách liên tục.



Hình 3: Nguyên lý hoạt động của tính năng Replication trong DFS

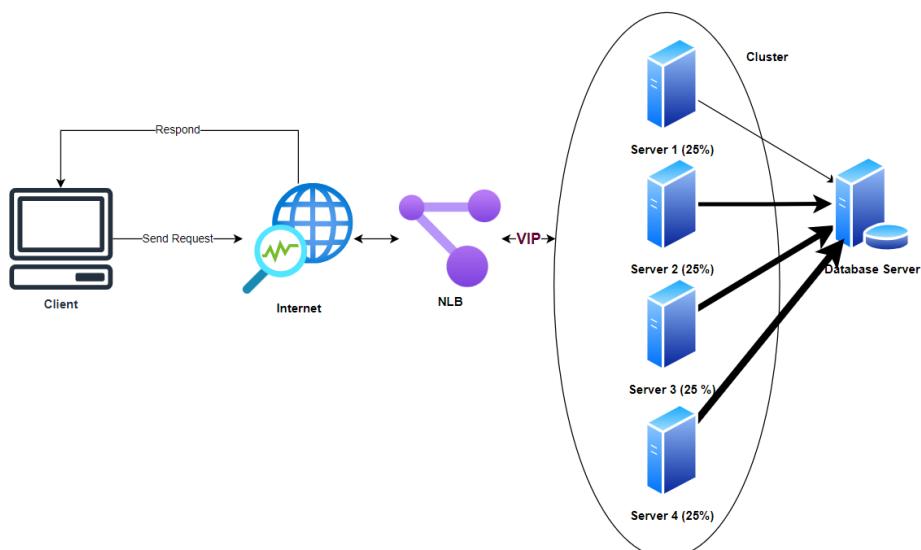
Để hoàn thành nội dung thực hành này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 3](#) trang 581 - 596. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 4.



Hình 4: Minh họa kiến trúc hệ thống mạng cho nội dung thực hành 3

4. Cấu hình cân bằng tải trong hệ thống mạng (Network Load Balancing)

Network Load Balancer (NLB) trong Windows Server là một dịch vụ cung cấp khả năng cân bằng tải cho các ứng dụng mạng, giúp cải thiện hiệu suất và tính sẵn sàng cao. NLB hoạt động bằng cách phân phối lưu lượng mạng đến nhiều máy chủ trong một cụm (cluster).

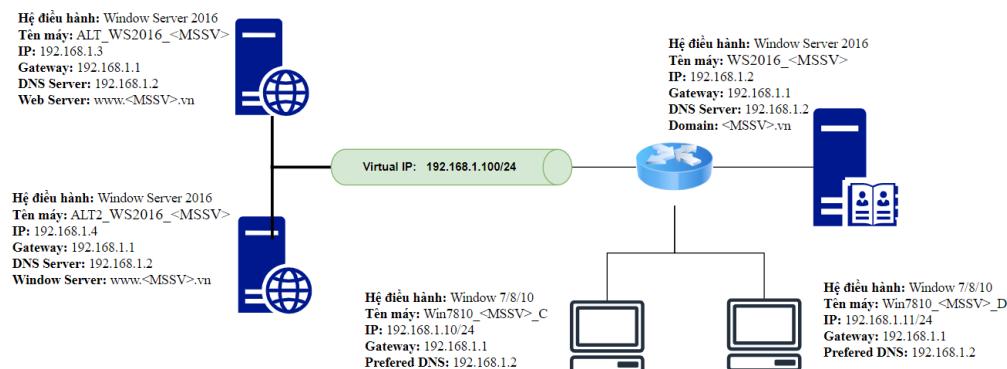


Hình 5: Minh họa nguyên lý hoạt động của NLB

Khi một yêu cầu mạng đến, NLB sử dụng các thuật toán như round-robin, weighted round-robin hoặc Least Connections để quyết định máy chủ nào sẽ xử lý yêu cầu đó,

đảm bảo không có máy chủ nào bị quá tải. Mỗi máy chủ trong cụm NLB được cấu hình với cùng một địa chỉ IP ảo (virtual IP - VIP), mà người dùng sẽ kết nối đến, trong khi NLB sẽ xác định máy chủ vật lý nào sẽ nhận yêu cầu. Nếu một máy chủ bị lỗi hoặc không phản hồi, NLB tự động loại bỏ máy chủ đó ra khỏi cụm và chuyển hướng lưu lượng đến các máy chủ còn lại, đảm bảo dịch vụ không bị gián đoạn. NLB có thể được cấu hình để xử lý các giao thức TCP, UDP và hỗ trợ các ứng dụng yêu cầu duy trì trạng thái kết nối ổn định.

Virtual IP (VIP) là một thành phần quan trọng trong cấu trúc của NLB trong Windows Server. VIP là địa chỉ IP mà các client sử dụng để kết nối với các dịch vụ của NLB do NLB tự động sinh ra làm vai trò “cầu nối” giữa client với cụm các máy chủ. Thay vì kết nối trực tiếp đến một máy chủ cụ thể, các client kết nối đến VIP, và NLB sẽ chịu trách nhiệm phân phối lưu lượng này đến các máy chủ trong cụm.



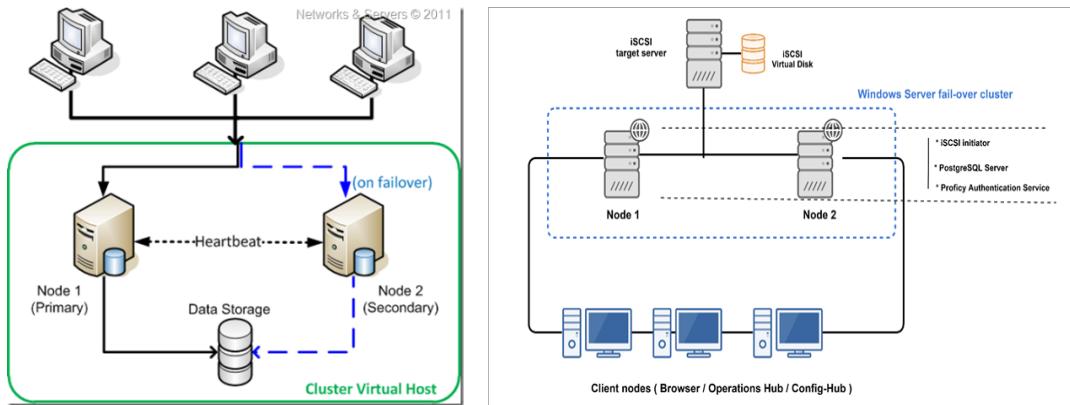
Hình 6: Minh họa kiến trúc hệ thống mạng cho nội dung thực hành 4

Để hoàn thành nội dung thực hành này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 4](#) trang 548 - 581. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 6.

5. Cài đặt và cấu hình Failover Clustering

Failover Clustering trong Windows Server là một công nghệ cung cấp khả năng sẵn sàng cao và khả năng chịu lỗi cho các ứng dụng và dịch vụ quan trọng. Nó hoạt động bằng cách nhóm nhiều máy chủ (gọi là nodes) thành một cluster để đảm bảo rằng nếu một node bị lỗi, các dịch vụ và ứng dụng đang chạy trên node đó sẽ tự động chuyển sang một node khác trong cluster mà không gây gián đoạn cho người dùng. Các nodes trong cluster chia sẻ dữ liệu và trạng thái thông qua một hệ thống lưu trữ chung (Data Storage / Virtual Disk) và liên lạc với nhau để theo dõi tình trạng của từng node. Khi một lỗi xảy ra, cơ chế failover sẽ ngay lập tức kích hoạt, chuyển dịch vụ từ node bị lỗi

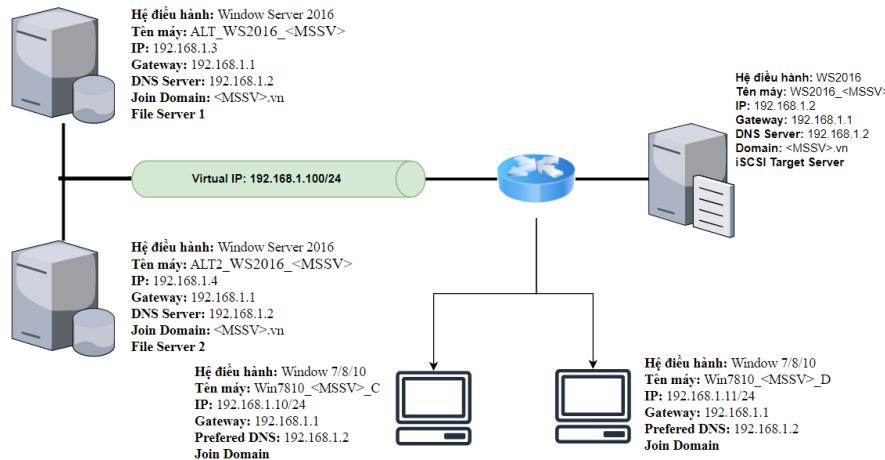
sang node hoạt động (theo heartbeat), giúp duy trì tính liên tục của hoạt động kinh doanh và giảm thiểu thời gian chết.



Hình 7: Minh họa nguyên lý hoạt động của Failover Clustering

Trong một Failover Cluster, iSCSI và File Server là hai thành phần quan trọng giúp cung cấp các dịch vụ và tài nguyên đối với các ứng dụng và người dùng cuối.

- iSCSI (Internet Small Computer System Interface) là một giao thức cho phép các máy chủ kết nối với các hệ thống lưu trữ từ xa thông qua mạng IP. Trong một Failover Cluster, iSCSI được sử dụng để kết nối các node trong cluster với các hệ thống lưu trữ chia sẻ dữ liệu. Điều này đảm bảo rằng dữ liệu có thể được truy cập và chia sẻ một cách đồng nhất giữa các node trong cluster, và khi một node chuyển tiếp, kết nối iSCSI sẽ tự động chuyển sang node mới.



Hình 8: Minh họa kiến trúc hệ thống mạng cho nội dung thực hành 5

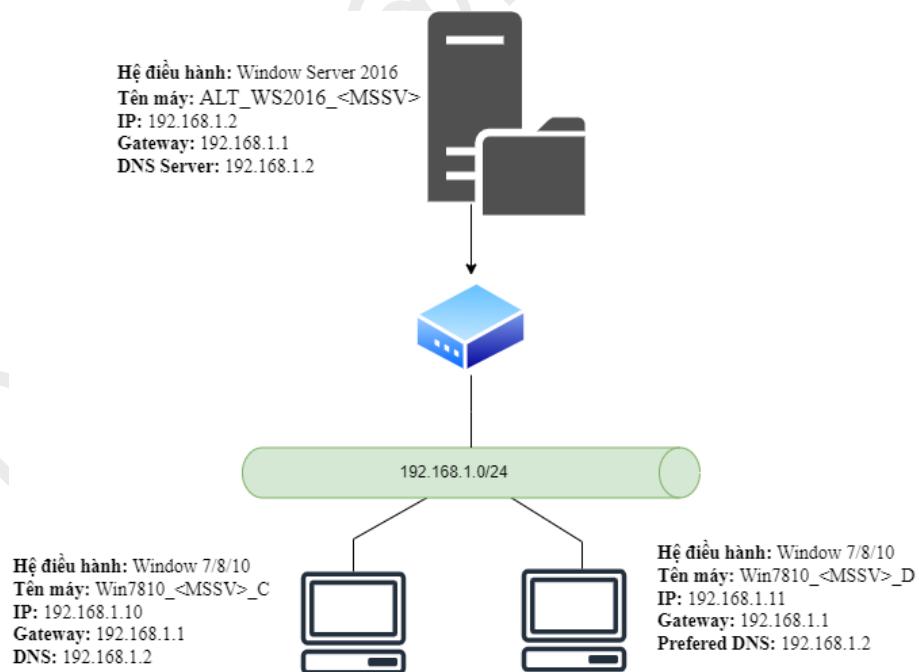
- File Server là dịch vụ cung cấp khả năng chia sẻ và quản lý tập tin và thư mục trên mạng. Trong một Failover Cluster, File Server thường được triển khai để cung cấp tài nguyên lưu trữ chia sẻ cho người dùng và ứng dụng. Bằng cách triển khai File Server trong một Failover Cluster, nếu một node gặp sự cố, dịch vụ File

Server sẽ tự động chuyển sang một node khác trong cluster mà không làm gián đoạn truy cập tài nguyên của người dùng.

Để hoàn thành nội dung thực hành này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong Tài liệu tham khảo 4 trang 581 - 645. Lưu ý sinh viên cần tuân theo các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 8.

6. Sao lưu và phục hồi dữ liệu sử dụng Window Server Backup

Windows Server Backup (WSB) là một tính năng tích hợp trong Windows Server, cung cấp giải pháp sao lưu và khôi phục dữ liệu cho hệ thống, ổ đĩa, phân vùng và tệp tin. WSB hỗ trợ sao lưu toàn bộ hệ thống (Full Backup), sao lưu gia tăng (Incremental Backup) và sao lưu theo lịch trình, giúp bảo vệ dữ liệu khỏi mất mát do lỗi phần cứng, tấn công mạng hoặc thao tác sai. Công cụ này cho phép khôi phục dữ liệu nhanh chóng, bao gồm khôi phục tệp riêng lẻ, khôi phục toàn bộ hệ thống thông qua Windows Recovery Environment (WinRE) hoặc khôi phục trạng thái hệ thống (System State). Ngoài ra, WSB có thể sao lưu dữ liệu lên ổ cứng cục bộ, mạng chia sẻ hoặc thiết bị lưu trữ ngoài, tuy nhiên không hỗ trợ trực tiếp sao lưu lên đám mây.



Hình 9: Minh họa kiến trúc hệ thống mạng cho nội dung thực hành 6

Để hoàn thành nội dung thực hành này, sinh viên sẽ thực hiện theo các yêu cầu và hướng dẫn trong [Tài liệu tham khảo 4](#) trang 646 - 681. Lưu ý sinh viên cần tuân theo

các giá trị sẽ được ánh xạ tương ứng như trong bảng 1 và phải thực hành các bước dựa trên kiến trúc mạng máy tính như trong hình 8.

III. Quy định bài thực hành

1. Sinh viên cần trình bày bài làm theo file template được GV cung cấp.
2. Nộp lại trên hệ thống LMS theo đúng deadline và các quy định liên quan.
3. Không chấp nhận những bài làm có dấu hiệu sao chép giống nhau và sẽ cho 0 điểm bài LAB của những bài làm này.

----HẾT----