BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC BÀ RỊA - VŨNG TÀU

KHOA KỸ THUẬT-CÔNG NGHỆ

ĐỒ ÁN TỐT NGHIỆP

ĐỀ TÀI: THIẾT KẾ HỆ THỐNG MẠNG CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ

Trình độ đào tạo: Đại học	**Hệ đào tạo:** Chính quy
Ngành: Kỹ thuật – Công nghệ	**Chuyên ngành:** Công nghệ thông tin
Khoá học: 2021	**Lớp:** DH21CT2
Giảng viên hướng dẫn:	ThS. Phạm Tuấn Trinh
Sinh viên thực hiện:	Võ Văn Thưởng – 21030873

Vũng Tàu, tháng 08 năm 2024

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

1. Về tinh thần thái độ và tác phong:.....

.....

.....

2. Về kiến thức chuyên môn: .....

.....

.....

3. Về nhận thức thực tế:.....

.....

.....

4. Về khả năng ứng dụng lý thuyết vào thực tế: .....

.....

.....

5. Đánh giá khác: .....

.....

.....

6. Các hướng nghiên cứu của đề tài có thể tiếp tục phát triển cao hơn: .....

.....

.....

7. Kết quả: Đạt ở mức nào (hoặc không đạt):.....

.....

.....

Bà Rịa - Vũng Tàu, ngày tháng năm 20

Giảng viên hướng dẫn

NHẬN XÉT CỦA GIẢNG VIÊN PHẢN BIỆN

1. Về tinh thần thái độ và tác phong:.....

.....

.....

2. Về kiến thức chuyên môn: .....

.....

.....

3. Về nhận thức thực tế:.....

.....

.....

4. Về khả năng ứng dụng lý thuyết vào thực tế: .....

.....

.....

5. Đánh giá khác: .....

.....

.....

6. Các hướng nghiên cứu của đề tài có thể tiếp tục phát triển cao hơn: .....

.....

.....

7. Kết quả: Đạt ở mức nào (hoặc không đạt):.....

.....

.....

Bà Rịa - Vũng Tàu, ngày tháng năm 20

Giảng viên phản biện

MỤC LỤC

MỤC LỤC HÌNH ẢNH

DANH MỤC BẢNG BIỂU

LỜI CẢM ƠN

Với lòng biết ơn sâu sắc nhất, em xin chân thành cảm ơn tập thể quý thầy cô Khoa Kỹ thuật - Công nghệ, chuyên ngành công nghệ thông tin đã ân cần giảng dạy, truyền đạt kiến thức, kinh nghiệm. Chính những kiến thức quý báu mà thầy cô đã truyền đạt là nguồn tư liệu quý giá để em hoàn thành tốt quá trình làm đồ án tốt nghiệp này.

Em cũng xin gửi làm cảm ơn đến Thầy Phạm Tuấn Trinh – người đã tận tình hướng dẫn em hoàn thành bài báo cáo đồ án tốt nghiệp này trong thời gian qua.

Trong quá trình làm báo cáo đồ án tốt nghiệp, dù em đã rất cố gắng cẩn thận nhưng cũng khó tránh khỏi những sai sót, em rất mong nhận được ý kiến đóng góp từ thầy, cô để em học thêm được nhiều kinh nghiệm làm báo cáo tốt hơn trong tương lai. Đồng thời do trình độ lý luận cũng như khả năng nghiên cứu, nhìn nhận vấn đề của em còn nhiều hạn chế, nên em cũng rất mong nhận được những ý kiến góp ý của các thầy, cô để em có thể hoàn thiện hơn về các kiến thức lĩnh hội thực tế.

Em xin chân thành cảm ơn!

LỜI MỞ ĐẦU

Trong thời đại công nghệ số phát triển mạnh mẽ như hiện nay, việc xây dựng một hệ thống mạng ổn định, hiệu quả và bảo mật là yếu tố quan trọng giúp doanh nghiệp duy trì hoạt động kinh doanh liên tục và nâng cao năng lực cạnh tranh. Đặc biệt đối với các doanh nghiệp vừa và nhỏ, việc thiết kế và triển khai một hệ thống mạng phù hợp không chỉ giúp tối ưu hóa quy trình làm việc mà còn tạo nền tảng vững chắc cho sự phát triển bền vững trong tương lai.

Mặc dù các doanh nghiệp vừa và nhỏ thường có nguồn lực hạn chế, nhưng với sự phát triển của các giải pháp công nghệ ngày nay, họ hoàn toàn có thể xây dựng được hệ thống mạng mạnh mẽ, linh hoạt và tiết kiệm chi phí. Đề tài "Thiết kế hệ thống mạng cho doanh nghiệp vừa và nhỏ" sẽ tập trung vào việc phân tích và triển khai các thành phần của một hệ thống mạng tối ưu, đảm bảo khả năng kết nối liên tục, bảo mật và mở rộng trong tương lai. Qua đó, nghiên cứu này sẽ đề xuất các giải pháp thiết thực giúp các doanh nghiệp vừa và nhỏ có thể ứng dụng công nghệ thông tin một cách hiệu quả và tối ưu.

Với mục tiêu nâng cao hiệu quả vận hành và tiết kiệm chi phí, bài viết sẽ đi sâu vào việc khảo sát nhu cầu thực tế của doanh nghiệp, phân tích các yêu cầu kỹ thuật, và đưa ra phương án thiết kế phù hợp, đáp ứng các tiêu chí về hiệu suất, bảo mật và khả năng mở rộng trong môi trường kinh doanh hiện đại.

Qua quá trình tìm hiểu, em đã được học hỏi và áp dụng những kiến thức và kỹ năng chuyên môn của mình để có thể xây dựng được một hệ thống mạng. Em đã tìm hiểu về cách hoạt động của một hệ thống mạng, các tính năng cơ bản cũng như các thuật ngữ liên quan đến lĩnh vực mạng. Đồng thời, em cũng được học hỏi về quy trình thiết kế và triển khai hệ thống mạng cho doanh nghiệp.

CHƯƠNG I: CƠ SỞ LÝ THUYẾT

I. Khái niệm và phân loại mạng máy tính

1. Khái niệm về mạng máy tính

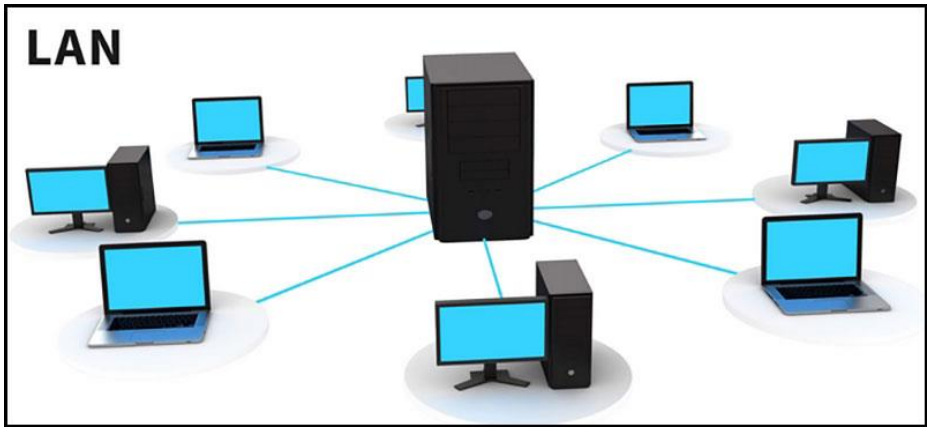
❖ Mạng máy tính là một hệ thống được tạo ra bằng cách kết nối các máy tính với nhau để chúng có thể giao tiếp và chia sẻ thông tin. Một mạng máy tính bao gồm các thiết bị máy tính như PC, laptop, máy chủ, máy in, điện thoại thông minh và các thiết bị mạng khác. Các máy tính trong mạng được kết nối với nhau bằng cáp mạng hoặc kết nối không dây. Khi được kết nối, chúng có thể gửi và nhận dữ liệu qua mạng. Mạng máy tính cho phép chúng ta gửi email, truy cập vào các trang web, chia sẻ tệp tin và in ấn từ bất kỳ máy tính nào trong mạng.

2. Phân loại mạng máy tính

❖ Mạng máy tính có thể được phân loại dựa trên nhiều tiêu chí khác nhau. Một số phân loại phổ biến của mạng máy tính:

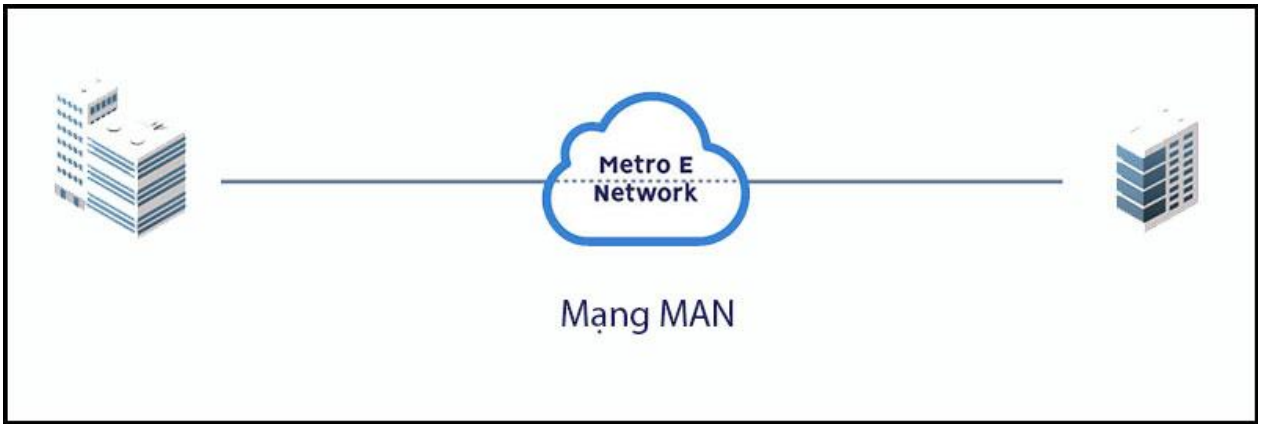
➢ Phân loại theo quy mô:

- **Mạng LAN (Local Area Network)**: hay còn được gọi là mạng cục bộ được dùng trong khu vực giới hạn nhất định như một phòng, một tòa nhà hay một khuôn viên, tốc độ truyền tải cao. Các thiết bị sử dụng mạng LAN có thể chia sẻ tài nguyên với nhau, mà điển hình là chia sẻ tập tin, máy in,... và một số thiết bị khác.



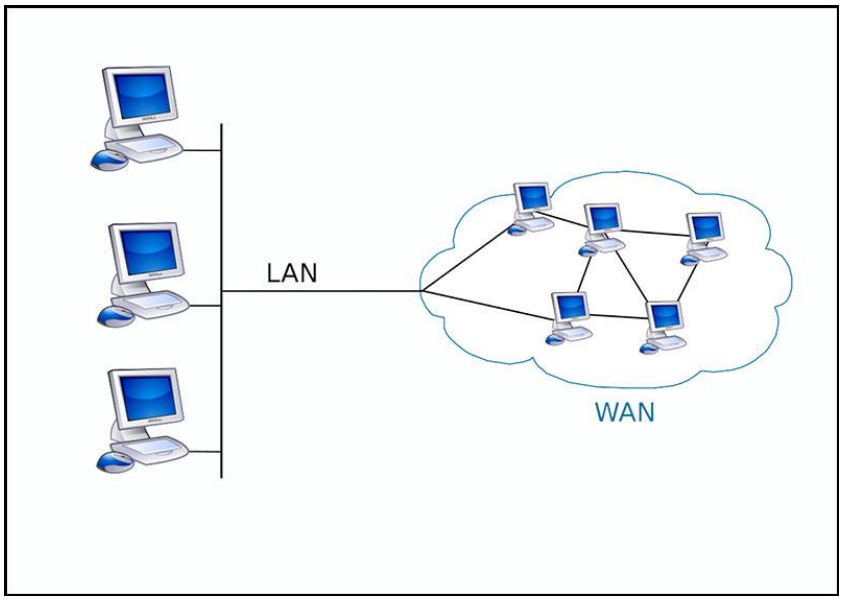
Hình 1: Mô hình hoạt động của mạng LAN

- **Mạng MAN (Metropolitan Area Network)**: Hay còn gọi là mạng đô thị liên kết từ nhiều mạng LAN qua dây cáp, các phương tiện truyền dẫn khác,..Mạng kết nối các máy tính trong cùng một thành phố hay một khu vực đô thị, một thị trấn, thành phố, tỉnh. Thường được dùng chủ yếu cho đối tượng là tổ chức, doanh nghiệp nhiều chi nhánh, nhiều bộ phận kết nối với nhau. Mạng Man thường được sử dụng cho doanh nghiệp vì mô hình này này cung cấp nhiều loại dịch vụ như kết nối đường truyền qua voice (thoại), data (dữ liệu), video(hình ảnh), triển khai các ứng dụng dễ dàng.



Hình 2: Mô hình hoạt động của mạng MAN

- **Mạng WAN (Wide Area Network)**: hay còn gọi là mạng diện rộng được kết hợp giữa các mạng đô thị bao gồm cả mạng MAN và mạng LAN thông qua thiết bị vệ tinh, cáp quang, cáp dây điện. Mạng diện rộng được tạo ra nhằm kết nối trên một diện lớn có quy mô trên quốc gia. Giao thức sử dụng trong mạng WAN là TCP/IP, đường truyền băng thông thay đổi tùy vào vị trí lắp đặt.



Hình 3: Mô hình hoạt động của mạng WAN

- **Wireless Network (Mạng không dây):** Là mạng điện thoại hoặc mạng máy tính sử dụng sóng radio làm sóng truyền dẫn hay tầng vật lý. Một mạng không dây là một mạng máy tính sử dụng các kết nối dữ liệu không dây giữa các nút mạng.

Hình 4: Mô hình hoạt động của mạng không dây

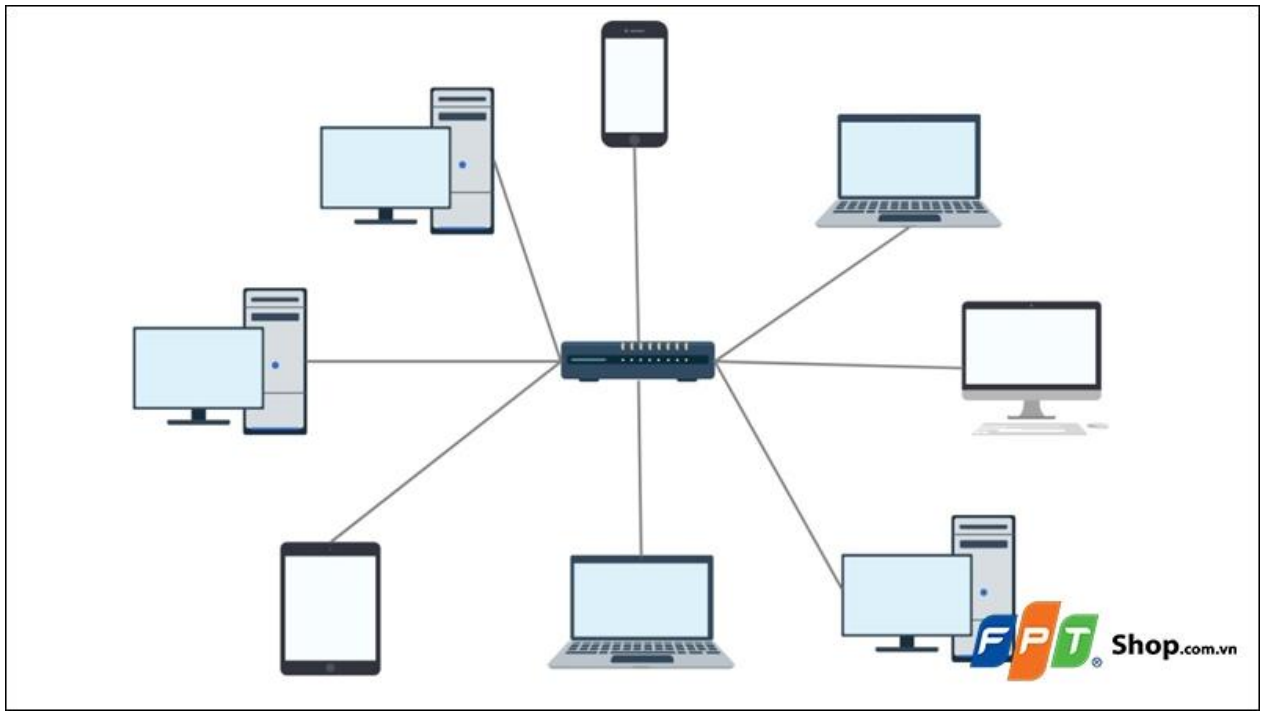
II. Khái niệm về Topology và các dạng Topology

1. Khái niệm về Topology

❖ Topology của mạng là cấu trúc hình học không gian mà thực chất là cách bố trí phần tử của mạng cũng nh cách nối giữa chúng với nhau. Thông thờng mạng có 3 dạng cấu trúc là: Mạng dạng hình sao (Star Topology), mạng dạng vòng (Ring Topology) và mạng dạng tuyến (Linear Bus Topology). Ngoài 3 dạng cấu hình kể trên còn có một số dạng khác biến tớng từ 3 dạng này nh mạng dạng cây, mạng dạng hình sao - vòng, mạng hỗn hợp,v.v....

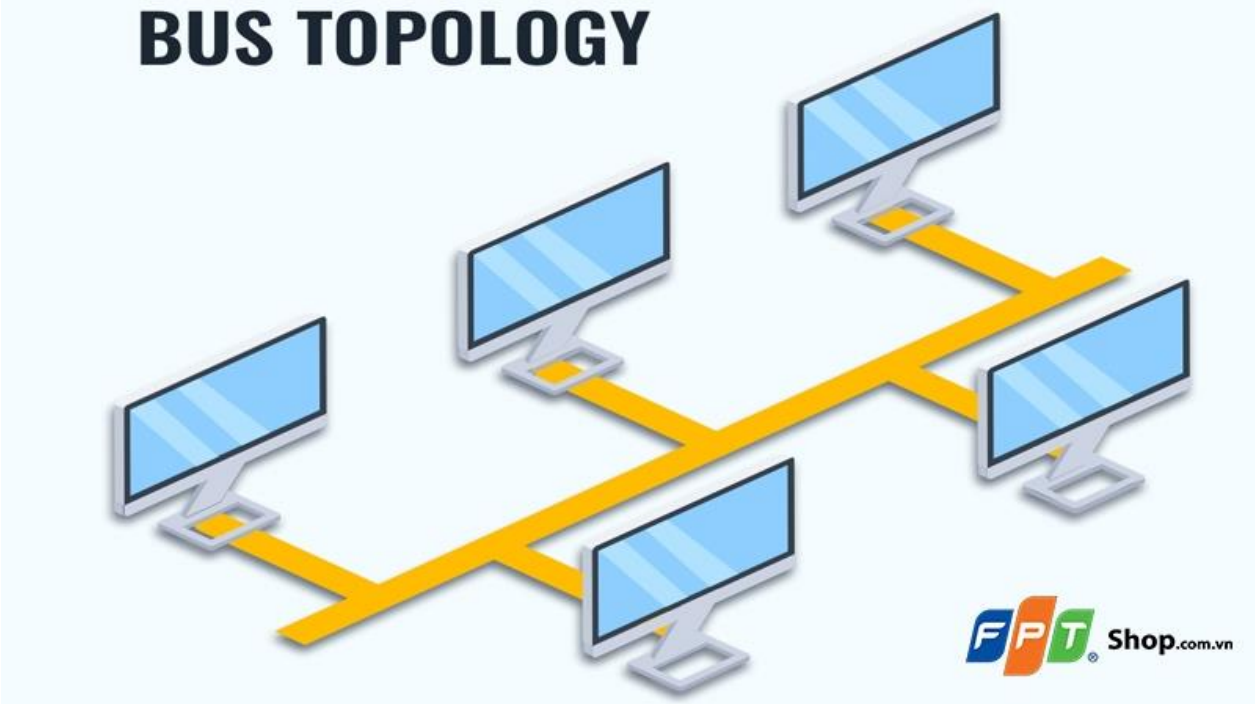
2. Các dạng Topology

❖ **Mạng dạng hình sao (Star topology)**: Mạng có một thiết bị trung tâm kết nối với các thiết bị khác theo hình sao. Loại mạng này dễ cài đặt và quản lý, nhưng nếu thiết bị trung tâm gặp sự cố thì toàn bộ mạng sẽ bị ngừng hoạt động.



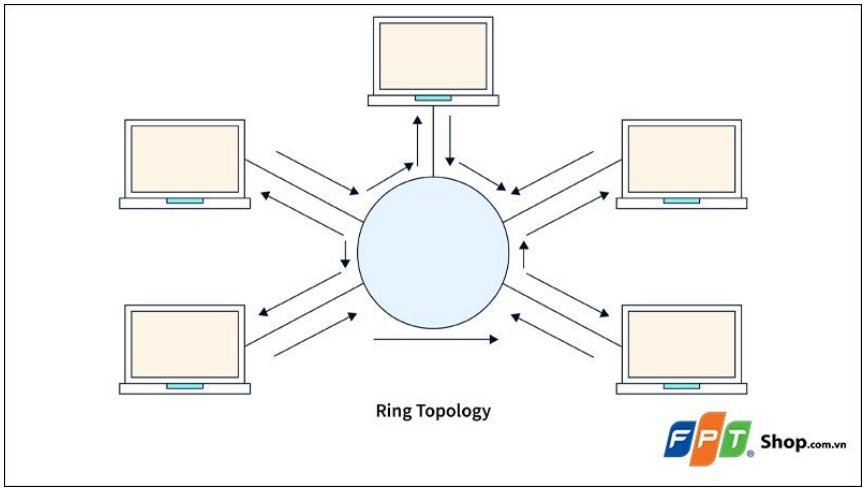
Hình 5: Mô hình hoạt động của mạng hình sao

❖ **Mạng tuyến tính (Bus Network)**: Mạng có một cáp chính kết nối các thiết bị theo dạng tuyến tính. Loại mạng này dễ cài đặt và tiết kiệm chi phí, nhưng có hiệu suất thấp và khó xử lý khi có sự cố.



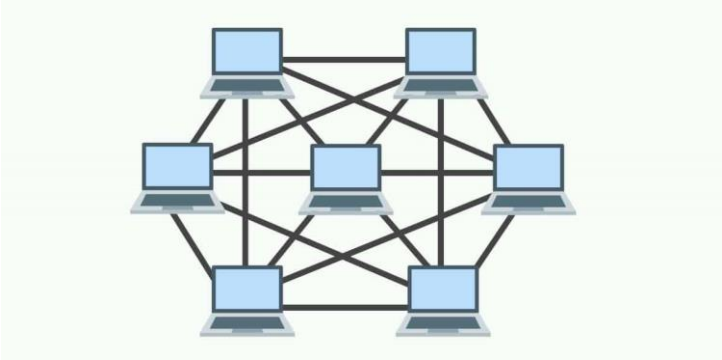
Hình 6: Mô hình hoạt động của mạng tuyến tính

❖ **Mạng hình vòng (Ring Network)**: Mạng có các thiết bị kết nối với nhau theo hình vòng tròn. Loại mạng này có hiệu suất cao và không bị nhiễu, nhưng khó cài đặt và khó xử lý khi có sự cố.



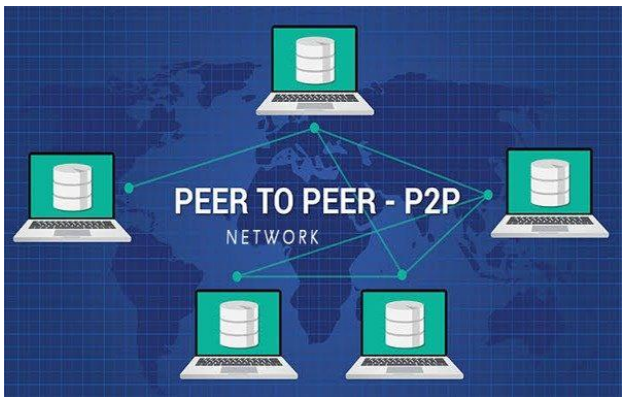
Hình 7: Mô hình hoạt động của mạng hình vòng

❖ **Mạng kết hợp (Mesh Network)**: Mạng có các thiết bị kết nối với nhau theo nhiều đường khác nhau. Loại mạng này có độ tin cậy cao và dễ mở rộng, nhưng tốn nhiều chi phí và khó quản lý.



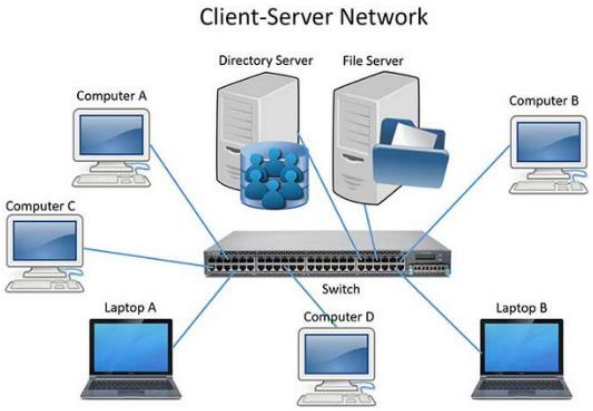
Hình 8: Mô hình hoạt động của mạng kết hợp

❖ **Mạng ngang hàng (Peer-to-Peer Network)**: Mạng có các máy tính kết nối với nhau mà không cần máy chủ trung gian. Loại mạng này dễ cài đặt và không phụ thuộc vào máy chủ, nhưng an ninh thấp và khó quản lý.



Hình 9: Mô hình hoạt động của mạng ngang hàng

❖ **Mạng khách chủ (Client-Server Network)**: Mạng có các máy chủ cung cấp dịch vụ cho các máy khách truy cập vào mạng. Loại mạng này có an ninh cao và dễ quản lý, nhưng tốn nhiều chi phí và phụ thuộc vào máy chủ.

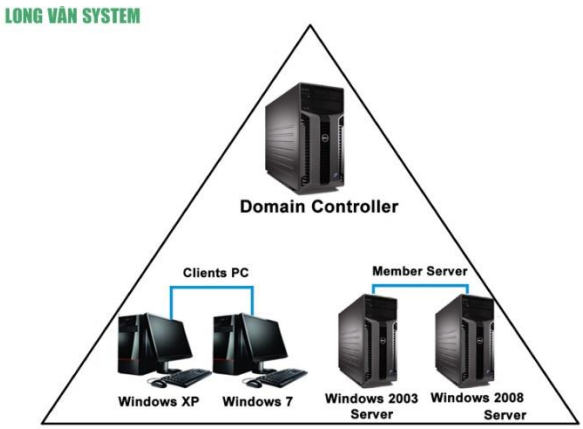


Hình 10: Mô hình hoạt động của mạng khách chủ

❖ **Mô hình mạng Workgroup**: Mô hình quản lý mạng không có máy chủ tập trung, mà các máy tính tự quản lý tài nguyên của mình và chia sẻ cho các máy khác trong cùng nhóm làm việc. Mô hình này thích hợp cho các mạng nhỏ và đơn giản.

Hình 11: Mô hình hoạt động của mạng Workgroup

❖ **Mô hình mạng Domain**: Mô hình quản lý mạng có máy chủ tập trung quản lý tài nguyên và người dùng của toàn bộ mạng. Mô hình này thích hợp cho các mạng lớn và phức tạp.



Hình 12: Mô hình hoạt động của mạng Domain

III. Các thành phần của hệ thống mạng máy tính

Một hệ thống mạng máy tính bao gồm nhiều thành phần khác nhau hoạt động cùng nhau để cho phép các thiết bị truyền thông với nhau. Dưới đây là một số thành phần chính:

❖ **Thiết bị đầu cuối:** Đây là các thiết bị được sử dụng để truy cập mạng, chẳng hạn như máy tính, máy in, điện thoại…

❖ **Thiết bị mạng**: Đây là các thiết bị giúp kết nối các thiết bị đầu cuối với nhau và với internet. Một số thiết bị mạng phổ biến bao gồm:

- **Bộ chuyển mạch:** Bộ chuyển mạch kết nối các thiết bị với nhau trong một mạng cục bộ (LAN).
- **Bộ định tuyến:** Bộ định tuyến kết nối các mạng khác nhau với nhau, chẳng hạn như mạng gia đình với internet, mạng văn phòng với internet,....
- **Modem:** viết tắt của Modulator and Demodulator - Bộ điều giải, là một thiết bị điều chế sóng tín hiệu tương tự để mã hóa dữ liệu số, và giải điều chế tín hiệu mạng để giải mã tín hiệu số. Giải thích một cách dễ hiểu hơn thì modem biến đổi thông tin kỹ thuật số từ các thiết bị kết nối mạng (máy tính, điện thoại) thành tín hiệu analog có

thể truyền qua dây dẫn, và ngược lại, modem dịch các tín hiệu analog thành dữ liệu số mà những thiết bị như máy tính có thể hiểu được.

- **Điểm truy cập không dây (WAP):** WAP cho phép các thiết bị kết nối với mạng bằng Wi-Fi.

❖ **Môi trường truyền dẫn:** Đây là phương tiện vật lý mà qua đó dữ liệu được truyền qua mạng. Một số môi trường truyền dẫn phổ biến bao gồm:

- **Cáp xoắn đôi:** Cáp xoắn đôi là loại cáp được sử dụng phổ biến nhất để kết nối các thiết bị trong mạng LAN.
- **Cáp quang:** Cáp quang sử dụng tia sáng để truyền dữ liệu và cung cấp tốc độ truyền nhanh hơn so với cáp xoắn đôi.
- **Sóng vô tuyến:** Sóng vô tuyến có thể được sử dụng để truyền dữ liệu qua khoảng cách xa mà không cần cáp.

❖ **Ứng dụng mạng**: Ứng dụng mạng là các chương trình được sử dụng để thực hiện các tác vụ trên mạng, chẳng hạn như gửi email, duyệt web và chia sẻ tệp.

IV. Các thành phần của hệ thống mạng máy tính

Giao thức mạng là tập hợp các quy tắc được thiết lập nhằm xác định cách để định dạng, truyền và nhận dữ liệu sao cho các thiết bị mạng máy tính - từ server và router tới endpoint - có thể giao tiếp với nhau. Các giao thức mạng cũng xác định các quy tắc và quy ước giao tiếp giữa các node phần mềm và phần cứng trên mạng. Các giao thức mạng phải được xác nhận và cài đặt bởi người gửi và người nhận để đảm bảo quá trình giao tiếp dữ liệu/mạng diễn ra suôn sẻ, được bảo mật và quản lý. Một số giao thức mạng phổ biến hiện nay là:

❖ **Internet Protocol Suite (bộ giao thức liên mạng)**: là tập hợp các giao thức thực thi protocol stack (chồng giao thức) mà Internet chạy trên đó. Internet Protocol Suite đôi khi được gọi là bộ giao thức TCP/IP. TCP và IP là những giao thức quan trọng trong Internet Protocol Suite - Transmission Control Protocol (TCP) và Internet Protocol (IP).

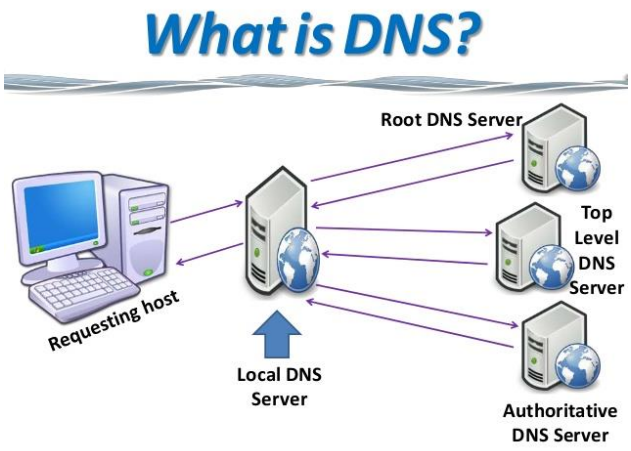
- **Transmission Control Protocol (TCP)**: là giao thức cốt lõi của Internet Protocol Suite. Transmission Control Protocol bắt nguồn từ việc thực thi mạng, bổ sung cho Internet Protocol. TCP cung cấp một phương thức phân phối đáng tin cậy một luồng octet (khối dữ liệu có kích thước 8 bit) qua mạng IP. Đặc điểm chính của TCP là khả năng đưa ra lệnh và kiểm tra lỗi. Tất cả các ứng dụng Internet lớn như World Wide Web, email và truyền file đều dựa vào TCP.
- **Internet Protocol (IP):** là giao thức chính trong Internet protocol suite để chuyển tiếp dữ liệu qua mạng. Chức năng định tuyến của Internet Protocol về cơ bản giúp thiết lập Internet. Giao thức tầng mạng thông dụng nhất ngày nay là Ipv4 hoặc Ipv6.
- **Hypertext Transfer Protocol (HTTP):** là nền tảng giao tiếp dữ liệu cho World Wide Web. HTTP là giao thức truyền tải siêu văn bản. Chúng là một trong năm giao thức chuẩn của mạng Internet. Giao thức này dùng để liên hệ thông tin giữa máy cung cấp dịch vụ (Web server) và Máy sử dụng dịch vụ (Web client).
- **File Transfer Protocol (FTP):** là giao thức truyền tải tệp tin. FTP cho phép người dùng truyền hoặc nhận các file từ xa qua một máy tính có kết nối với internet. FTP có khả năng chuyển file giữa các máy tính có hệ điều hành khác nhau.
- **Simple Mail Transfer Protocol (SMTP):** là giao thức truyền tải thư đơn giản. SMTP là tiêu chuẩn công nghiệp cho việc truyền email giữa các máy tính qua internet hoặc các mạng khác. SMTP chỉ xử lý việc gửi email, không xử lý việc nhận email. Để nhận email, người dùng cần sử dụng các giao thức khác như POP3 hoặc IMAP. SMTP sử dụng cổng 25 để giao tiếp với các máy chủ email khác. SMTP cũng sử dụng cổng 587 để giao tiếp với các máy khách email (email client) như Outlook, Thunderbird, v.v. SMTP là một giao thức văn bản đơn giản, có thể đọc được bởi con người. SMTP sử dụng các lệnh và phản hồi để thiết lập phiên giao tiếp và truyền tải email. Mỗi lệnh và phản hồi bao gồm một mã số và một thông điệp mô tả.

V. Các dịch vụ của hệ thống mạng máy tính

- **Domain Controller**: Domain Controller (DC) là một máy chủ đóng vai trò quan trọng trong hệ thống Active Directory (AD) của Microsoft. Nó lưu trữ cơ sở dữ liệu AD, cung

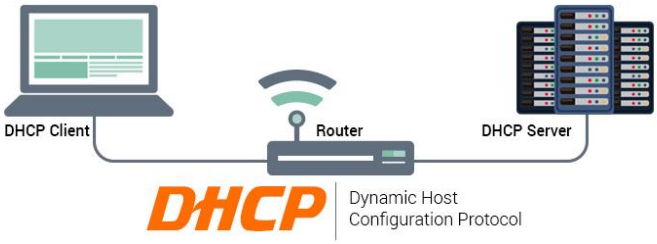
cấp dịch vụ xác thực và ủy quyền cho người dùng và máy tính trong miền, đồng thời quản lý các chính sách và cấu hình cho toàn bộ miền.

- **DNS:**Viết tắt của Domain Name System, là hệ thống phân giải tên miền thành các địa chỉ IP tương ứng và ngược lại. Khi bạn nhập một tên miền vào trình duyệt web, trình duyệt sẽ gửi một yêu cầu đến máy chủ DNS. Máy chủ DNS sẽ tra cứu tên miền trong cơ sở dữ liệu của nó và trả về địa chỉ IP tương ứng. Sau đó, trình duyệt sẽ sử dụng địa chỉ IP này để kết nối với trang web.



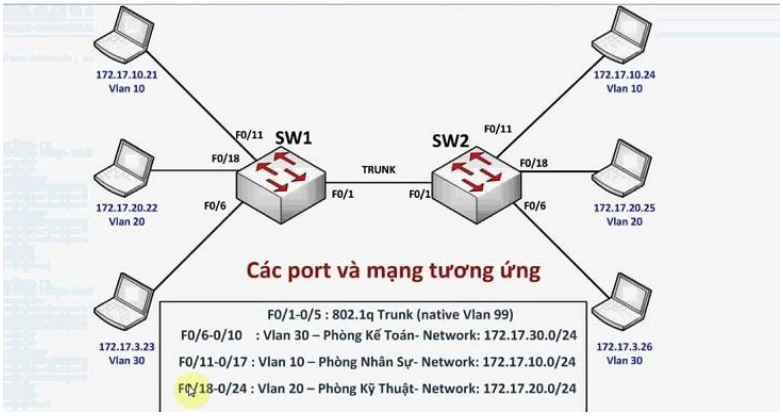
Hình 13: Dịch vụ DNS

- **DHCP:** Viết tắt của Dynamic Host Configuration Protocol, là dịch vụ cấp phát động các thông số cấu hình mạng cho các thiết bị yêu cầu, như địa chỉ IP, subnet mask, default gateway, DNS server... và các thông số cấu hình mạng khác cho các thiết bị (client) trên mạng.



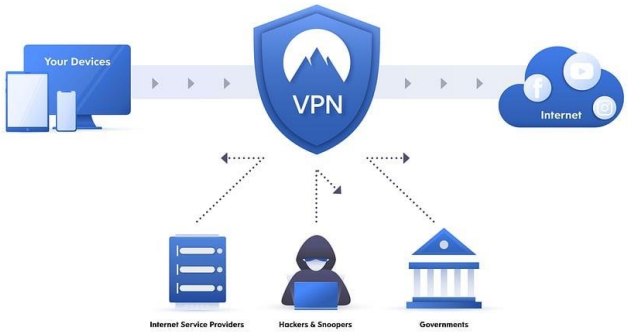
Hình 14: Dịch vụ DHCP

❖ **VLAN:** Là viết tắt của Virtual Local Area Network, hay còn gọi là Mạng LAN ảo. VLAN là một kỹ thuật phân chia mạng LAN vật lý thành các mạng logic riêng biệt, được gọi là các VLAN. Mạng LAN ảo được tạo ra bằng cách gán thẻ các khung Ethernet với một mã VLAN.



Hình 15: Dịch vụ VLAN

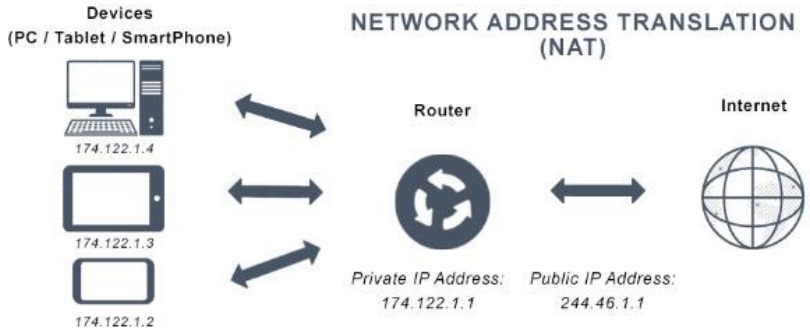
❖ **VPN:** Là viết tắt của Virtual Private Network, hay Mạng riêng ảo. Nó là một dịch vụ giúp bạn kết nối với internet thông qua một máy chủ trung gian, che giấu địa chỉ IP thực của bạn và mã hóa dữ liệu của bạn. Điều này giúp bạn ẩn danh trực tuyến và bảo vệ quyền riêng tư của bạn. Khi bạn kết nối với VPN, thiết bị của bạn sẽ tạo ra một đường hầm được mã hóa đến máy chủ VPN. Dữ liệu của bạn sau đó được truyền qua đường hầm này đến internet, khiến cho nó không thể đọc được bởi bất kỳ ai theo dõi kết nối của bạn. VPN hoạt động nhờ vào sự kết hợp với các giao thức đóng gói PPTP, L2TP, IPSec, GRE, MPLS, SSL, TLS.



Hình 16: Dịch vụ VPN

- Các loại VPN:
  - **Site-to-Site VPN**: là mô hình dùng để kết nối các hệ thống mạng ở các nơi khác nhau tạo thành một hệ thống mạng thống nhất. Ở loại kết nối này thì việc chứng thực an đầu phụ thuộc vào thiết bị đầu cuối ở các Site, các thiết bị này hoạt động như Gateway và đây là nơi đặt nhiều chính sách bảo mật nhằm truyền dữ liệu một cách an toàn giữa các Site.
  - **Remote Access VPN**: hay còn được gọi là Client-to-Site, là loại này thường áp dụng cho nhân viên làm việc lưu động hay làm việc ở nhà muốn kết nối vào mạng công ty một cách an toàn. Cũng có thể áp dụng cho văn phòng nhỏ ở xa kết nối vào Văn phòng trung tâm của công ty. Remote Access VPN còn được xem như là dạng User-to-LAN, cho phép người dùng ở xa dùng phần mềm VPN Client kết nối với VPN Server.

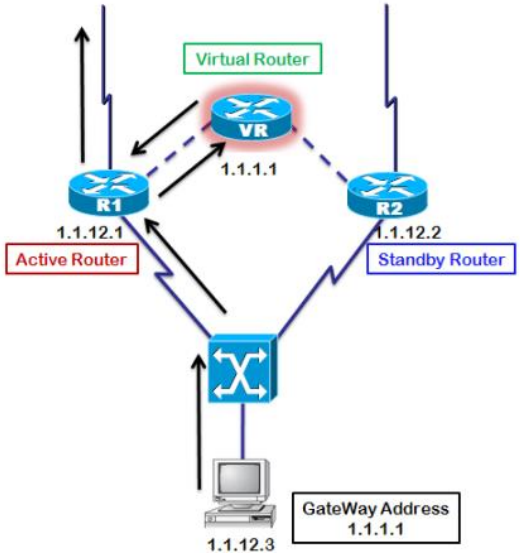
❖ **NAT:** Là viết tắt của Network Address Translation, hay Dịch địa chỉ mạng. Đây là kỹ thuật cho phép một hoặc nhiều địa chỉ IP nội bộ (private IP) được chuyển đổi thành một hoặc nhiều địa chỉ IP công cộng (public IP) trước khi truyền dữ liệu ra Internet. NAT hoạt động như một "người phiên dịch" giữa mạng nội bộ và Internet. Khi một thiết bị trong mạng nội bộ muốn truy cập Internet, NAT sẽ chuyển đổi địa chỉ IP nội bộ của thiết bị đó thành địa chỉ IP công cộng của bộ định tuyến. Sau đó, bộ định tuyến sẽ gửi yêu cầu đến Internet. Khi dữ liệu được trả về từ Internet, NAT sẽ chuyển đổi địa chỉ IP công cộng trong gói dữ liệu thành địa chỉ IP nội bộ của thiết bị đích.



Hình 17: Dịch vụ NAT

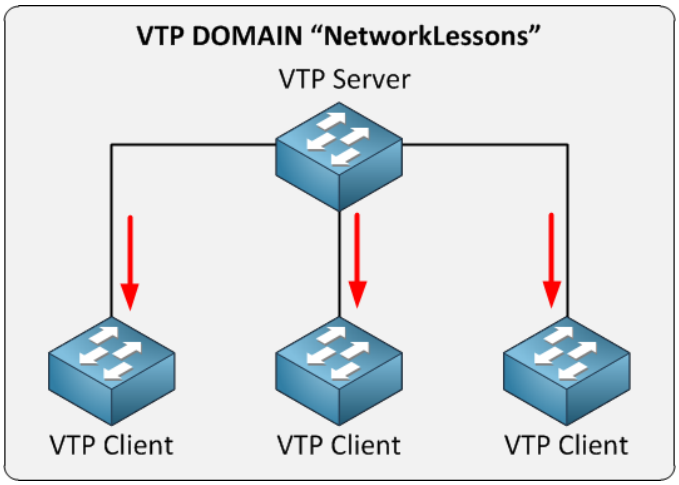
- Các loại NAT:
  - **NAT tĩnh (Static NAT)**: NAT tĩnh luôn ánh xạ một địa chỉ IP nội bộ cố định sang một địa chỉ IP công cộng cố định.
  - **NAT động (Dynamic NAT)**: NAT động ánh xạ một địa chỉ IP nội bộ động sang một địa chỉ IP công cộng được chọn ngẫu nhiên từ một nhóm địa chỉ IP công cộng.
  - **NAT cổng(NAT Overload)**: NAT cổng ánh xạ một số cổng TCP hoặc UDP cụ thể sang một địa chỉ IP nội bộ cụ thể.

❖ **HSRP:** Giao thức HSRP (Hot Standby Router Protocol) là một giao thức dự phòng được sử dụng trong mạng máy tính để cung cấp sự dự phòng cho các thiết bị định tuyến. Mục tiêu chính của HSRP là tạo ra một thiết bị chính (active router) và một hoặc nhiều thiết bị dự phòng (standby router) để đảm bảo tính sẵn sàng và liên tục của mạng. Khi sử dụng HSRP, các thiết bị định tuyến được cấu hình để tạo thành một nhóm, trong đó một thiết bị được chọn làm active router và các thiết bị khác trong nhóm sẽ là các standby router. Khi thiết bị active router gặp sự cố (ví dụ: mất kết nối mạng), một trong các thiết bị standby router sẽ chuyển thành active router ngay lập tức, giữ cho mạng vẫn hoạt động mà không có sự gián đoạn đáng kể. Quá trình này được thực hiện tự động bởi các thiết bị trong nhóm HSRP, giúp cải thiện tính sẵn sàng và tin cậy của mạng.



Hình 18: Dịch vụ HSRP

❖ **VTP:** VTP (VLAN Trunking Protocol) là một giao thức được sử dụng trong mạng Ethernet để quản lý và cấu hình các VLAN (Virtual Local Area Networks) trên các switch trong một mạng LAN (Local Area Network). Chức năng chính của VTP bao gồm: đơn giản hóa quản lý VLAN và đồng bộ hóa cấu hình VLAN trên các switch trong mạng LAN, giúp tăng cường tính nhất quán và quản lý hiệu quả.



Hình 19: Dịch vụ VTP

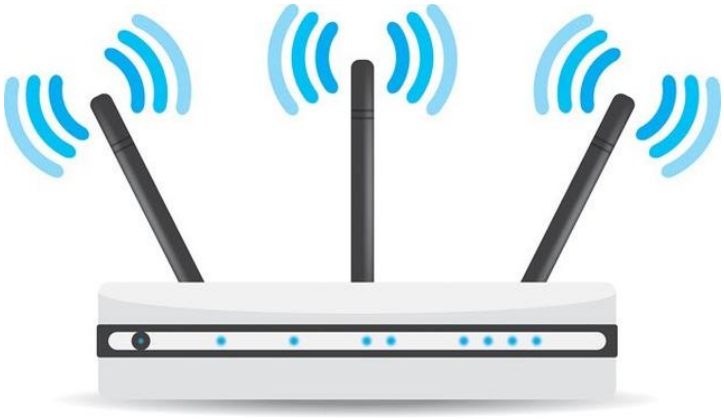
❖ **File Server:** Là dịch vụ lưu trữ và chia sẻ các tập tin trên mạng. Tạo các thư mục chia sẻ (Shared Folder) cho các phòng ban trong công ty, như kế toán, nhân sự, kỹ thuật... Phân quyền truy cập (Permission) cho các thư mục chia sẻ theo nhóm người dùng.

VI. Các thiết bị kết nối mạng

- **NIC**: là một cụm từ viết tắt của "Network Interface Card". NIC là một thiết bị phần cứng (hardware) hoặc một thành phần tích hợp trên máy tính hoặc thiết bị mạng khác, giúp kết nối máy tính hoặc thiết bị đó với mạng máy tính. NIC thường bao gồm một cổng hoặc kết nối vật lý để kết nối với cáp mạng, và nó có chức năng điều chỉnh và truyền dữ liệu giữa máy tính và mạng.

Hình 20: Thiết bị NIC

- **Router:** Hay còn gọi là bộ định tuyến, là thiết bị mạng có chức năng chuyển tiếp gói dữ liệu giữa các mạng máy tính. Router hoạt động dựa trên bảng định tuyến để xác định đường đi tốt nhất cho các gói dữ liệu.



Hình 21: Thiết bị router

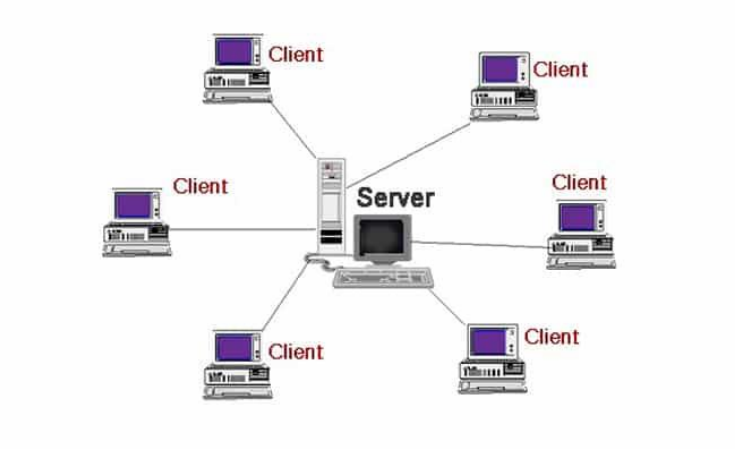
❖ **Switch:** Hay còn gọi là bộ chuyển mạch, là thiết bị mạng có chức năng kết nối các thiết bị mạng với nhau trong cùng một mạng LAN (mạng cục bộ). Switch hoạt động dựa trên địa chỉ MAC của các thiết bị để chuyển tiếp khung dữ liệu đến đúng đích.

Hình 22: Thiết bị Switch

❖ **Server:** Hay còn gọi là máy chủ, là một hệ thống máy tính được thiết kế để cung cấp các dịch vụ, tài nguyên và dữ liệu cho các máy tính khác trong mạng. Server có thể là một máy tính riêng lẻ hoặc một cụm máy tính được kết nối với nhau.

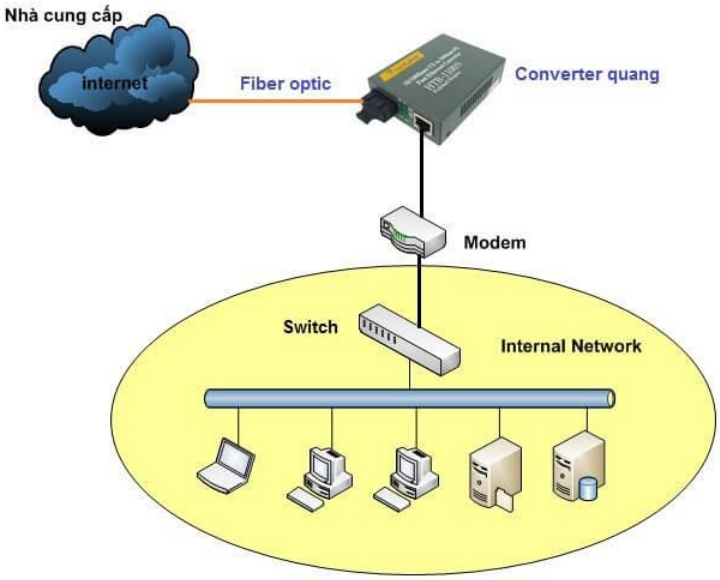
Hình 23: Máy chủ - Server

❖ **Client:** là một hoặc nhiều máy tính được sử dụng trong mạng máy tính để truy cập các dịch vụ được cung cấp bởi máy chủ (Server)



Hình 24: Thiết bị Client

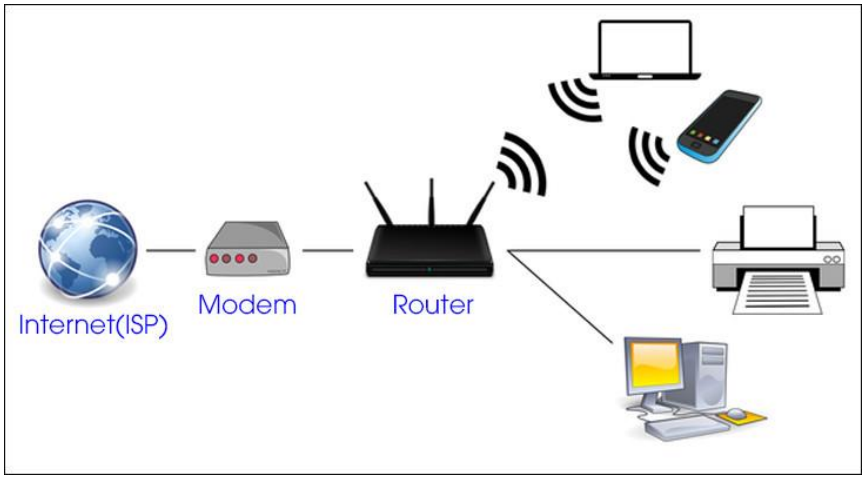
❖ **Converter (bộ chuyển đổi):** là thiết bị điện tử được sử dụng để chuyển đổi tín hiệu giữa các loại cáp mạng khác nhau hoặc giữa các loại tín hiệu khác nhau trong hệ thống mạng. Converter đóng vai trò quan trọng trong việc kết nối các thiết bị mạng khác nhau và mở rộng phạm vi truyền dẫn dữ liệu**.**



Hình 25: Thiết bị Converter

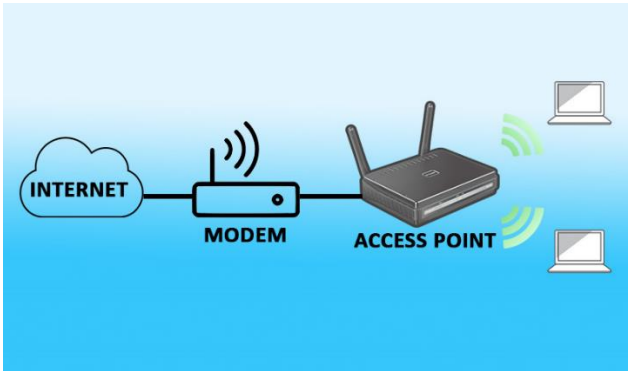
- Có hai loại converter chính:
  - **Converter quang - điện**: Chuyển đổi tín hiệu điện từ cáp mạng đồng sang tín hiệu quang để truyền dẫn qua cáp quang hoặc ngược lại. Converter quang-điện được sử dụng phổ biến trong hệ thống mạng cáp quang do khả năng truyền dẫn dữ liệu với tốc độ cao và khoảng cách xa hơn so với cáp mạng đồng.
  - **Converter media**: Chuyển đổi tín hiệu giữa các loại cáp mạng đồng khác nhau, ví dụ như từ cáp UTP sang cáp RJ45 hoặc cáp BNC. Converter media được sử dụng để kết nối các thiết bị mạng cũ với các thiết bị mạng mới hoặc để kết nối các mạng LAN khác nhau.
- Ngoài ra, còn có một số loại converter khác:
  - **Converter công nghiệp**: Được sử dụng trong môi trường công nghiệp khắc nghiệt, có khả năng chống bụi bẩn, độ ẩm và nhiệt độ cao.
  - **Converter PoE (Power over Ethernet)**: Cung cấp nguồn điện cho các thiết bị mạng qua cáp Ethernet, giúp loại bỏ nhu cầu sử dụng nguồn điện riêng cho các thiết bị này.
  - **Converter SFP**: Cung cấp khả năng kết nối linh hoạt cho các thiết bị mạng, cho phép người dùng sử dụng các loại cáp quang và module quang khác nhau.

❖ **Modem (modulator và demodulator):** là thiết bị mã hóa và giải mã các xung điện). Modem đóng vai trò giao tiếp với mạng lưới của các nhà cung cấp dịch vụ Internet (ISP) thông qua hệ thống cáp nối đồng trục, cáp quang, đường dây điện thoại (DSL). Modem chuyển đổi tín hiệu Internet từ dạng analog thành dạng kỹ thuật số để sử dụng trên thiết bị điện tử. Bên cạnh đó, Modem WiFi còn tích hợp thêm chức năng phát Wi-Fi, cho phép các thiết bị không dây kết nối và truy cập Internet qua sóng Wi-Fi.



Hình 26: Thiết bị Modem

❖ **Access Point (AP):** hay còn gọi là điểm truy cập hoặc bộ phát Wifi, là một thiết bị mạng thu-phát Wifi có thể tạo ra một mạng không dây cục bộ (WLAN). Access Point thường được dùng tại môi trường công sở, nhà hàng, tiệc cưới hay các tòa nhà lớn nhằm tạo ra không gian sử dụng mạng rộng rãi mà không làm suy giảm tốc độ của mạng. Một chức năng ưu việt của Access Point đó là khả năng liên kết các máy tính tại nơi làm việc, từ đó sẽ giúp việc kiểm soát và truyền tải dữ liệu trở nên đơn giản hơn.



Hình 27: Thiết bị Acces Point

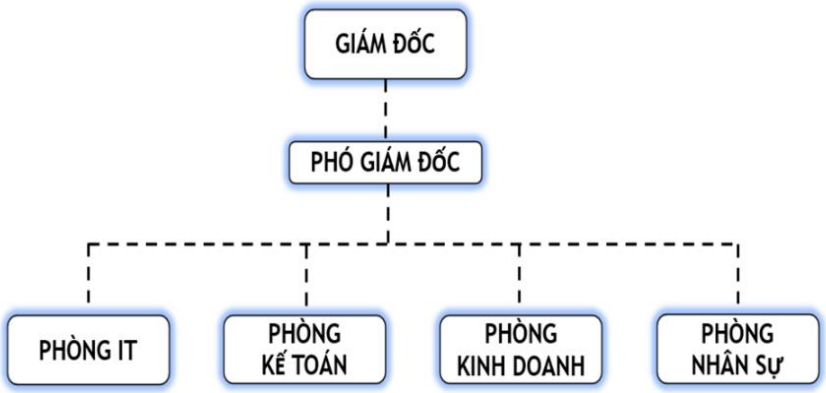
VII. Các chức năng và ứng dụng của hệ thống mạng máy tính

- Hệ thống mạng máy tính là sự kết hợp của nhiều máy tính, thông qua thiết bị kết nối mạng cùng với các phương tiện truyền thông theo một cấu trúc. Mục đích của việc này là nhằm chia sẻ thông tin và trao đổi dữ liệu giữa các thiết bị trong cùng một hệ thống. Trong đó, phương tiện truyền thông chính là giao thức mạng và môi trường truyền dẫn.
- Các chức năng và ứng dụng của hệ thống mạng máy tính có thể bao gồm:
  - Cho phép người dùng chia sẻ, sử dụng mọi tài nguyên chung như chương trình, thiết bị dữ liệu,… mà không cần phải quan tâm đến vị trí thực của tài nguyên và người dùng.
  - Dễ dàng xem, chỉnh sửa, sao chép tập tin từ một máy tính khác như đang thực hiện trên chính máy tính của mình.
  - Trong cùng hệ thống mạng, các máy tính và thiết bị có thể sử dụng chung tài nguyên thiết bị lưu trữ (HDD, SSD, ổ đĩa CD), máy in, máy fax, modem, máy quét, webcam cùng nhiều thiết bị khác.
  - Có thể sao chép dữ liệu từ máy này sang máy khác hoặc lưu dữ liệu tập trung ở máy chủ, để người dùng mạng máy tính có thể truy cập bất cứ khi nào cần.
  - Chia sẻ máy in, bộ nhớ, các ổ đĩa và nhiều thiết bị khác để người dùng có thể dùng chung.
  - Cài đặt phần mềm dùng chung để tiết kiệm chi phí.
  - Có thể trao đổi thông tin giữa các máy tính thông qua phần mềm trò chuyện trực tuyến (chat) hoặc thư điện từ (email).
  - Dữ liệu lưu trữ qua các phần mềm mạng máy tính sẽ đảm bảo tính an toàn cao hơn so với việc lưu trữ trên máy tính cá nhân.
  - Có khả năng truy và xuất các chương trình dữ liệu từ xa.
  - Việc trao đổi thông tin cũng như tài liệu gián tiếp khá dễ dàng, nhanh chóng.

CHƯƠNG II: XÂY DỰNG HỆ THỐNG MẠNG CHO CÁC DOANH NGHIỆP VỪA VÀ NHỎ

I. Mô hình thực tế của các doanh nghiệp vừa và nhỏ

- Qua thời gian thực tập ở công ty TNHH Tiến Thịnh và khảo sát qua một số doanh nghiệp khác thì em xây dựng mô hình hệ thống mạng theo cấu trúc của các công ty bao gồm 1 tầng trệt và 1 lầu.
- Qua khảo sát các doanh nghiệp đa phần các doanh nghiệp có các phòng như sau: Phòng IT, Phòng Kế Toán, Phòng Kinh Doanh, Phòng Nhân Sự. Như vậy sơ đồ tổ chức cơ bản của các doanh nghiệp vừa và nhỏ như sau:

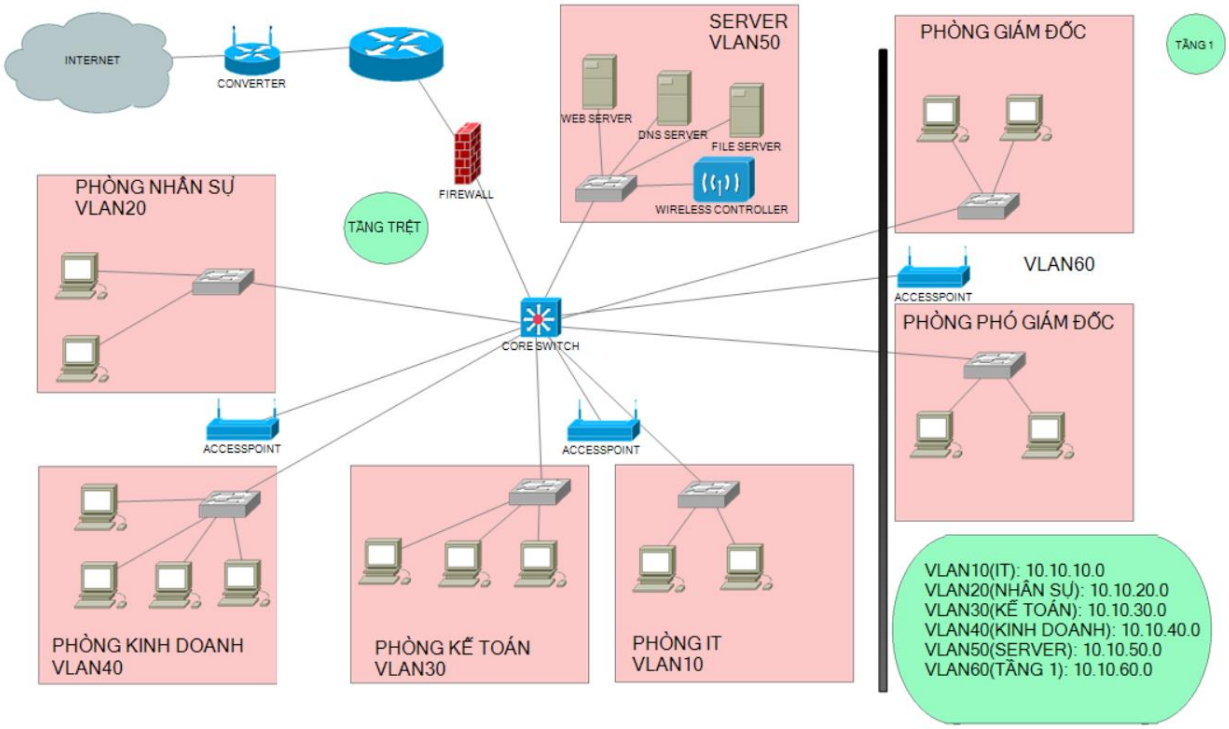


Hình 28: Sơ đồ tổ chức

- Kích thước của các phòng ban:
  - Phòng IT sẽ có khoảng 5 máy tính và 1 server, có thể nâng cấp lên 15 máy tính.
  - Phòng Kế Toán sẽ có khoảng 7 máy tính, có thể nâng cấp tối đa lên 15 máy tính.
  - Phòng Kinh Doanh sẽ có khoảng 10 máy tính, có thể nâng cấp lên 15 máy tính.
  - Phòng Nhân Sự sẽ có khoảng 5 máy tính, có thể nâng cấp lên 15 máy tính.

II. Thiết kế hệ thống mạng cho doanh nghiệp vừa và nhỏ

1. Thiết kế logic hệ thống mạng



Hình 29: Sơ đồ logic hệ thống mạng

2. Đặc tả của hệ thống mạng

- Dựa vào sơ đồ hệ thống logic hệ thống mạng và các thiết bị ta có thể phân tích như sau:
- Mạng được chia thành 2 khu vực chính: Tầng trệt và Tầng 1
  - Tầng trệt: Bao gồm các phòng: Phòng IT, Phòng Kinh Doanh, Phòng Kế Toán, Phòng Nhân Sự,
  - Tầng 1: Phòng Giám Đốc, Phòng Phó Giám Đốc
  - Mỗi phòng đều được chia VLAN cùng với địa chỉ IP riêng biệt để tiện cho việc quản lý và không xảy ra sự cố trùng lặp:
    - VLAN10(IT): 10.10.10.0/24 SM: 255.255.255.0
    - VLAN20(NHANSU): 10.10.20.0/24 SM: 255.255.255.0
    - VLAN30(KETOAN): 10.10.30.0/24 SM: 255.255.255.0
    - VLAN40(KINHDOANH): 10.10.40.0/24 SM: 255.255.255.0
    - VLAN50(TANG1): 10.10.50.0/24 SM: 255.255.255.0
    - VLAN60(SERVER): 10.10.60.0/24 SM: 255.255.255.0
- Mỗi khu vực được kết nối với nhau thông qua một bộ chuyển mạch (switch) 24 port, 100Mbps.
- Một bộ định tuyến (router) được sử dụng để kết nối mạng nội bộ với Internet.
- Tất cả thiết bị mạng đều tập trung về tủ rack 27U đặt ở phòng IT để quản lý.
- Hệ thống mạng bao gồm:
  - Switch Layer 2: chia đều cho mỗi phòng làm việc
  - Switch Core Layer 3: Active
  - Router: là nguồn kết nối các thiệt bị trong mạng LAN với mạng Internet.
  - Server để cấu hình các dịch vụ
  - Wireless Controller để cấu hình mạng không dây
  - Modem Wifi để kết nối mạng
- Hệ thống sử dụng mạng hình sao kết hợp với mô hình mạng khách chủ (Client-Server Network) để máy chủ cung cấp dịch vụ cho các máy khách truy cập vào mạng
- Access Point để chia sẻ Wifi giữa các tầng: 2 Access được đặt trung gian ở các phòng Kế Toán, Kinh Doanh, IT, Nhân Sự; 1 Access được đặt ở tầng 1
- Các Switch Core Layer 3 và Router đều đặt IP tĩnh

- Mỗi phòng đều có một bộ chuyển mạch (Switch Layer2) để kết nối với các Client trong phòng, đóng vai trò trung tâm trong việc kết nối các thiết bị đầu cuối trong mạng LAN (mạng cục bộ).
- Mỗi Switch Layer2 sẽ nối với Switch Core Layer3. Switch Core Layer3 có nhiệm vụ kết nối các Switch Layer 2 với nhau để chuyển tiếp các gói tin dữ liệu giữa các thiết bị mạng được kết nối với nó dựa trên địa chỉ MAC, chia mạng LAN thành các mạng con logic (VLAN) để tăng cường bảo mật và hiệu quả quản lý. Switch Layer 2 sẽ trunking để nhận VLAN tương ứng từ Switch Core Layer3.
- Switch Layer 3 sẽ nối với Router tương ứng, Router sẽ xác định đường đi cho các gói tin dữ liệu giữa các mạng khác nhau dựa trên địa chỉ IP. Đồng thời Router có nhiệm vụ kết nối mạng LAN với các mạng khác như Internet, WAN,... hoặc các mạng LAN ở Site khác.
- Router đều được kết nối với Converter để tạo mạng LAN hoặc Wifi cho các thiết bị. Converter nhận tín hiệu Internet từ nhà cung cấp dịch vụ (ISP) và chuyển đổi tín hiệu đó thành tín hiệu digital phù hợp với thiết bị mạng, cung cấp địa chỉ IP cho Router chuyên dụng của doanh nghiệp. Router nhận tín hiệu mạng từ Converter, sau đó sẽ chuyển dữ liệu đến thiết bị trong mạng nội bộ mà đã yêu cầu dữ liệu ban đầu.
- Server:
  - Nối với Switch Layer 2
  - Cấp VLAN riêng cho Server
  - Đặt Ip tĩnh: 10.10.50.100 SM: 255.255.255.0
  - Cấu hình các dịch vụ hệ thống: DHCP, DNS, Domain Controller, VPN,….
- Wireless Controller:
  - Nối với Switch Layer 2 chung Switch với Server
  - Đặt IP tĩnh: 10.10.2.100 SM: 255.255.255.0

❖ Các giao thức và cấu hình sử dụng trong hệ thống

- Trên Switch:
  - Tạo VLAN tương ứng với từng phòng ban trên Switch Core.
  - Cấu hình VTP trên một switch-core làm VTP server và các switch còn lại sẽ tự động nhận thông tin cấu hình VLAN từ server.
  - Cấu hình trunking để kết nối các switch với nhau để chuyển tiếp dữ liệu giữa các VLAN trên cả switch core và switch access.
  - Cấu hình rapid spanning-tree protocol để chống loop trên switch core.
  - Trên các switch access, ta sẽ cấu hình Spanning-Tree và cấu hình các portfast, port fast trunk đấu vào các thiết bị để hội tụ nhanh hơn, đồng thời bật tính năng bpduguard trên các port.
  - Đặt địa chỉ IP.
  - Cấu hình HSRP – dự phòng gateway để cung cấp sự dự phòng cho các thiết bị định tuyến.
  - Định tuyến động giao thứ EIGRP.
- Trên Router:
  - Cấu hình cơ chế NAT để hệ thống truy cập ra được internet.
  - Cấu hình VPN để hệ thống mạng có thể truy cập từ xa.
  - Mỗi tầng và phòng ban sẽ dùng DHCP để cấp IP cho các Client
  - Cấu hình định tuyến động EIGRP.
  - Đặt địa chỉ IP
- Trên Server:
  - Dựng Domain Controller để tạo User tương ứng với mỗi nhân viên khi đăng nhập.
  - Sử dụng dịch vụ NAT để giúp che giấu địa chỉ IP thực của các thiết bị trong mạng nội bộ khi truy cập Internet giúp cho việc khó bị tấn công từ bên ngoài.
  - Cấu hình DNS để phân giải địa chỉ IP thành tên miền của công ty
  - Các clients có thể sử dụng dịch vụ FTP để download/upload file từ/đến server.

3. Thiết bị mạng cần sử dụng

Bảng 1: Danh sách các thiết bị mạng cần sử dụng cho xây dựng hệ thống mạng

STT	Tên thiết bị	Hình ảnh	Mô tả
1	Router Cisco ISR4331-V/K9		- Mã sản phẩm: ISR4331-V/K9 - Tổng thông lượng: 100 Mbps đến 300 Mb / giây - Tổng số cổng WAN hoặc LAN 10/100/1000 trên bo mạch: 3 - Cổng dựa trên RJ-45: 2 - Cổng dựa trên SFP: 2 - Khe cắm mô-đun dịch vụ nâng cao (SM-X): 1 - Các khe NIM (Môđun Giao diện Mạng): 2 - Khe ISC trên bo mạch: 1 - Ký ức: 4 GB (mặc định) / 16 GB (tối đa) - Bộ nhớ flash: 4 GB (mặc định) / 16 GB (tối đa) - Tùy chọn cung cấp điện: Nội bộ: AC và PoE - Chiều cao rack: 1 RU - Kích thước (H x W x D): 44,45 x 438,15 x 438,15 mm - Gói trọng lượng: 12,96 Kg

2	Switch Layer 2 CISCO WS-C2960L-24TS-AP		- Hãng: Cisco - Mã sản phẩm: WS-C2960L-24TS-LL - Cổng giao tiếp: 24 port GigE, 4 x 1G SFP, LAN Lite - IOS: LAN Lite - Băng thông chuyển: 52 Gbps - Băng thông chuyển: 104 Gbps - 10/100/1000 Ethernet Ports: 24 - Giao diện Uplink: 4 x 1G SFP - Fanless: Y - DRAM: 512 MB - Bộ nhớ Flash: 256 MB - Kích thước (H x D x W): 1.73 x 9.45 x 17.5 in. (4.4 x 24 x 44.5 cm) - Net Cân nặng: 7.21 lb (3.27 kg) Bảo hành: 12 tháng
3	Switch Core Layer 3 CISCO WS-C3650-24TS-L		- Mã sản phẩm: WS-C3650-24TS-L - Bộ tính năng: LAN Base - Giao diện Uplink: 4 x 1G SFP - Cổng: 24 cổng 10/100/1000 Ethernet - Số xếp chồng tối đa: 9 - Stack băng thông: 160 Gpbs - Chuyển tiếp băng thông: 41,66Mpps - Chuyển đổi công suất: 88 Gb / giây - RAM: 4 G - Bộ nhớ flash: 2G - Số AP cho mỗi switch / stack: 25 - Kích thước: 44,5 cm x 44,5 cm x 4,4 cm - Trọng lượng: 17,49 Kg

4	Wireless Controller Cisco AIR-CT3504-K9		Là một thiết bị quản lý mạng không dây của Cisco Systems, được thiết kế để cung cấp quản lý tập trung và kiểm soát cho các mạng Wi-Fi trong môi trường doanh nghiệp. Nó cung cấp khả năng quản lý và điều khiển tập trung cho tối đa 150 điểm truy cập (AP) và 3000 thiết bị khách. * Thông số kĩ thuật: - 1x Gigabit Ethernet đa năng (lên đến 5 Gigabit Ethernet) - 4x Gigabit Ethernet - Bộ xử lý: Lõi kép 1 GHz - Bộ nhớ: 2 GB RAM - Khả năng hỗ trợ: Tối đa 150 AP Tối đa 3000 thiết bị khách Kích thước: 43,94 x 214,3 x 215,9 mm Khối lượng: 4,4lbs (2 kg)

5	Access Point Wi-Fi TP-Link EAP225 Gigabit AC1350 MU-MIMO		Dùng để phát sóng wifi các phòng. - **Wi-Fi Băng Tần Kép Nhanh:** Đồng thời 450 Mbps trên 2.4 GHz và 867 Mbps trên 5 GHz đồng thời, tổng cộng là 1317 Mbps tốc độ Wi-Fi. - **Chuẩn Wifi:** Wi-Fi 5 (802.11ac) - **Được tích hợp vào Omada SDN:** Zero-Touch Provisioning (ZTP), Quản lý cloud tập trung và Giám sát thông minh. - **Quản Lý Tập Trung:** Truy cập cloud và ứng dụng Omada để quản lý cực kỳ tiện lợi và dễ dàng. - **Chuyển Vùng Liền Mạch:** Ngay cả các luồng video và cuộc gọi thoại cũng không bị ảnh hưởng khi người dùng di chuyển giữa các vị trí - **Hỗ Trợ PoE:** Hỗ trợ cả chuẩn 802.3af / at và Passive PoE (bao gồm bộ chuyển đổi PoE) để cài đặt linh hoạt. - **Mạng Khách An Toàn:** Cùng với nhiều tùy chọn xác thực (SMS / Facebook Wi-Fi / Voucher, v.v.) và các công nghệ bảo mật không dây phong phú. - **Công Nghệ Không Dây Tiên Tiến:** Tối ưu hóa hiệu suất mạng với các công nghệ MU-MIMO, Band Steering, Airtime Fairness và Beamforming.

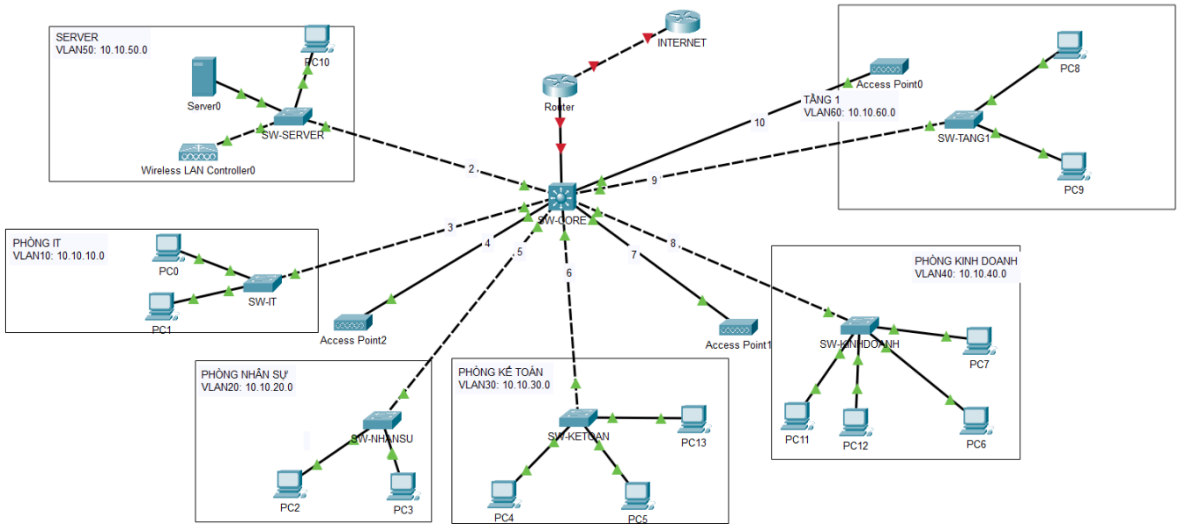
6	Tủ rack 27U		Tập trung các thiết bị mạng về một tủ để dễ quản lý hơn - Kích thước: 1410 x 600 x 1000 - Tải trọng: 500 - 800kg - Kết cấu khung: Quy cách tủ đứng, cửa lưới, tủ được thiết kế 2 khung chịu lực 6 thanh giằng đỡ khung - Phụ kiện: Thanh cấp nguồn 6 chấu đa năng chuẩn rack 19", bộ ốc cài bắt thiết bị 4 quạt tản nhiệt 20W. - Bên trong tủ rack có 1 ổ cắm nguồn 6 chấu - Hệ thống bánh xe và chân tăng giúp dễ di chuyển cũng như cố định tủ dễ dàng.
7	Patch panel		Đi dây cho tủ rack thêm tính thẩm mỹ Patch panel là một bảng cắm, thông qua đó các cáp sẽ kết nối các máy trong mạng LAN cho gọn gàng hơn so với việc cắm trực tiếp, đồng thời cũng dễ bảo quản và sửa chữa khi có sự cố. Tất cả các cáp mạng đi âm tường , một đầu nối với Office Box, đầu kia được đấu với PatchPanel

8	Thùng mạng cat 6 (200m)		Dùng để đi dây tới các máy tính, là cáp xoắn cặp, không bọc chống nhiễu (CAT6-UTP: Unshielded Twisted Pair Cable), gồm các dây dẫn đồng có bọc cách điện, hai dây dẫn được xoắn với nhau tạo thành một cặp và các cặp dây dẫn lại được xoắn với nhau để tạo thành cáp UTP; Hỗ trợ mạng ở tốc độ Gigabit Ethernet-đến 5000Mbps.
9	Cáp quang		Bao bọc bên ngoài là lớp vỏ bằng nhựa HDPE cứng cáp dày 1,2mm nhưng vẫn đảm bảo tính đàn hồi và chịu căng tốt. Bên trong là ống đệm lỏng và dây gia cường giúp cáp khi treo sẽ gánh được độ võng thấp nhất có thể.
10	Hạt mạng		Dùng để bấm vào 2 đầu dây mạng để truyền tín hiệu cho nhau
11	Máy trạm Server		Là một máy tính được nối mạng, quản lý tài nguyên của mạng, có IP tĩnh, có năng lực xử lý cao và trên máy đó người ta cài đặt các phần mềm dịch vụ để phục vụ cho các máy tính khác (máy trạm) truy cập để yêu cầu cung cấp các dịch vụ và tài nguyên.

CHƯƠNG III: CẤU HÌNH VÀ KIỂM THỬ HỆ THỐNG MẠNG DỰA TRÊN MÔ HÌNH

I. Cài đặt và cấu hình

- Sau khi xây dựng mô hình hệ thống mạng, bước tiếp theo chính là triển khai và cấu hình các giao thức và dịch vụ. Mục tiêu là đảm bảo cho hệ thống mạng vận hành mượt mà, hiệu quả và đi vào hoạt động một cách ổn định nhất.
- Sau khi lắp đặt dây và các thiết bị mạng, ta được sơ đồ như sau:



Hình 30: Sơ đồ lắp đặt dây mạng cho hệ thống

1. Cấu hình VLAN và giao thức VTP (VLAN Trunking Protocol)

- VLAN là một kỹ thuật để phân chia một mạng vật lý thành nhiều mạng logic khác nhau, mỗi mạng này hoạt động như một mạng riêng biệt, tách biệt. Điều này giúp quản lý, kiểm soát và bảo mật hiệu quả hơn.
- VTP là một giao thức được sử dụng trong mạng nội bộ để quản lý và cấu hình các VLAN trên các switch trong mạng LAN một cách tự động. Thay vì phải cấu hình VLAN trên từng switch một cách độc lập, VTP cho phép quản trị viên chỉ cần cấu hình một switch làm VTP server và các switch còn lại sẽ tự động nhận thông tin cấu hình VLAN từ server.
- Ta sẽ cấu hình VLAN và VTP trên Switch Core
- Trên Switch Core tạo các VLAN như sau:
  - VLAN2: wireless
  - VLAN10: it
  - VLAN20: nhansu
  - VLAN30: ketoan
  - VLAN40: kinhdoanh
  - VLAN50: server
  - VLAN60: tang1

❖ Mở SW-Core → vào tag CLI → gõ en → vào mode configure terminal

Switch> en	Chuyển vào chế độ Privileged
Switch# conf t	Chuyển vào chế độ Global Configuration
Switch (config)# hostname SW-Core	Cấu hình tên cho switch là SW-Core
SW-Core (config)# vtp domain doan	Tạo vtp domain cho SW-Core
SW-Core (config)# vtp mode server	Tạo SW-Core là mode server
SW-Core (config)# vlan 2	Tạo vlan 2
SW-Core (config – vlan)# name wireless	Tạo tên cho vlan 2 là wireless
SW-Core (config – vlan)#vlan 10	Tạo vlan 10
SW-Core (config – vlan)# name it	Tạo tên cho vlan 10 là it
SW-Core (config – vlan)# vlan 20	Tạo vlan 20
SW-Core (config – vlan)# name nhansu	Tạo tên cho vlan 20 là nhansu
SW-Core (config – vlan)#vlan 30	Tạo vlan 30
SW-Core (config – vlan)# name ketoan	Tạo tên cho vlan 30 là ketoan
SW-Core (config – vlan)# vlan 40	Tạo vlan 40
SW-Core (config – vlan)# name kinhdoanh	Tạo tên cho vlan 40 là kinhdoanh
SW-Core (config – vlan)# vlan 50	Tạo vlan 50
SW-Core (config – vlan)# name server	Tạo tên cho vlan 50 là server
SW-Core (config – vlan)# vlan 60	Tạo vlan 60
SW-Core (config – vlan)# name tang1	Tạo tên cho vlan 60 là tang1
SW-Core (config – vlan)#end	Chuyển về chế độ cấu hình Privileged

Bảng 2: Cấu hình VLAN và giao thức VTP

❖ Các switch access khác cấu hình VTP là client để nhận VLAN từ SW-Core

➢ SW-IT:

Switch>en	Chuyển về chế độ cấu hình Privileged
Switch# conf t	Chuyển vào chế độ Global Configuration
Switch (config)# hostname SW-IT	Cấu hình tên cho switch là SW-IT
SW-IT (config)# vtp domain doan	Tạo vtp domain cho SW-IT
SW-IT (config)# vtp mode client	Tạo SW-IT là mode client

➢ SW-NHANSU:

Switch>en	Chuyển về chế độ cấu hình Privileged
Switch# conf t	Chuyển vào chế độ Global Configuration
Switch (config)# hostname SW-NHANSU	Cấu hình tên cho switch là SW-NHANSU
SW-NHANSU (config)# vtp domain doan	Tạo vtp domain cho SW-NHANSU
SW-NHANSU (config)# vtp mode client	Tạo SW-NHANSU là mode client

➢ SW-KETOAN:

Switch>en	Chuyển về chế độ cấu hình Privileged
Switch# conf t	Chuyển vào chế độ Global Configuration
Switch (config)# hostname SW-KETOAN	Cấu hình tên cho switch là SW-KETOAN
SW-KETOAN (config)# vtp domain doan	Tạo vtp domain cho SW-KETOAN
SW-KETOAN (config)# vtp mode client	Tạo SW-KETOAN là mode client

- SW-KINHDOANH:

Switch>en	Chuyển về chế độ cấu hình Privileged
Switch# conf t	Chuyển vào chế độ Global Configuration
Switch (config)# hostname SW-KINHDOANH	Cấu hình tên cho switch là SW-KINHDOANH
SW-KINHDOANH (config)# vtp domain doan	Tạo vtp domain cho SW-KINHDOANH
SW-KINHDOANH (config)# vtp mode client	Tạo SW-KINHDOANH là mode client

- SW-SERVER:

Switch>en	Chuyển về chế độ cấu hình Privileged
Switch# conf t	Chuyển vào chế độ Global Configuration
Switch (config)# hostname SW-SERVER	Cấu hình tên cho switch là SW-SERVER
SW-SERVER (config)# vtp domain doan	Tạo vtp domain cho SW-SERVER
SW-SERVER (config)# vtp mode client	Tạo SW-SERVER là mode client

- SW-TANG1:

Switch>en	Chuyển về chế độ cấu hình Privileged
Switch# conf t	Chuyển vào chế độ Global Configuration
Switch (config)# hostname SW-TANG1	Cấu hình tên cho switch là SW-TANG1
SW-TANG1 (config)# vtp domain doan	Tạo vtp domain cho SW-TANG1
SW-TANG1 (config)# vtp mode client	Tạo SW-TANG1 là mode client

2. Cấu hình Trunking

- Trunking là một phương pháp được sử dụng để kết nối các switch với nhau để chuyển tiếp dữ liệu giữa các VLAN. Ta sẽ cấu hình trunking giữa các port trên switch để chuyển tiếp dữ liệu giữa các VLAN, đồng thời cung cấp khả năng đồng bộ hóa cấu hình VLAN giữa các switch. Như vậy ta sẽ cấu hình như sau:
  - Các port nối giữa các Switch Core và Switch Access sẽ là port trunk.
  - Port đấu giữa Switch với Server, Switch đấu với Client sẽ là port access và ta sẽ gán với những VLAN tương ứng.
  - Các port đấu với Wireless Controller, Access Point cũng sẽ là port trunk.
- SW-Core

SW-Core>en	Chuyển về chế độ cấu hình Privileged
SW-Core#conf t	Chuyển vào chế độ Global Configuration
SW-Core (config)# int range gig1/0/2 – 10	Chuyển cấu hình vào chế độ interface Gig1/0/2 đến Gig1/0/1-
SW-Core (config-if-range)# switchport mode trunk	Cho phép interface Gig1/0/2 đến Gig1/0/10 hoạt động ở chế độ trunk cố định và đồng thời tự động thương lượng để chuyển đổi trạng thái của đường liên kết thành trạng thái Trunk
SW-Core (config-if-range)# no shutdown	Mở port sang trạng thái mở
SW-Core (config-if-range)# end	Chuyển về chế độ cấu hình Privileged
SW-Core (config)# write	Lưu file cấu hình

Bảng 3: Cấu hình Trunking

- Tiếp theo, ta sẽ cấu hình port đấu giữa switch với Server, switch đấu với Client sẽ là port access và ta sẽ gán với những VLAN tương ứng.

❖ SW-SERVER

SW-SERVER> en	Chuyển về chế độ cấu hình Privileged
SW-SERVER# conf t	Chuyển vào chế độ Global Configuration
SW-SERVER (config)# int Fa0/4	Chuyển cấu hình vào chế độ interface Fa0/4
SW-SERVER (config-if)# sw access vlan 50	Gán port Fa0/4 vào VLAN 50
SW-SERVER (config-if)# exit	Thoát ra chế độ interface Fa0/4
SW-SERVER (config)# int gig0/1	Chuyển cấu hình vào chế độ interface Gig0/1
SW-SERVER (config-if)# switchport mode trunk	Cho phép interface Gi0/1 hoạt động ở chế độ trunk cố định và đồng thời tự động thương lượng để chuyển đổi trạng thái của đường liên kết thành trạng thái Trunk
SW-SERVER (config-if)# end	Thoát ra chế độ interface Gig0/1
SW-SERVER# write	Lưu file cấu hình

❖ SW-IT

SW-IT> en	Chuyển về chế độ cấu hình Privileged
SW-IT# conf t	Chuyển vào chế độ Global Configuration
SW-IT (config)# int range fa0/2-3	Chuyển cấu hình vào chế độ interface Fa0/2 đến Fa0/3
SW-IT (config-if-range)# sw access vlan 10	Gán các port từ port Fa0/2 đến Fa0/3 vào VLAN 10
SW-IT (config-if-range)# exit	Thoát ra chế độ interface Fa0/2 đến Fa0/3
SW-IT (config)# int gig0/1	Chuyển cấu hình vào chế độ interface Gig0/1
SW-IT (config-if)# sw mode trunk	Cho phép interface Gig0/1 hoạt động ở chế độ trunk cố định và đồng thời tự động thương lượng để chuyển đổi trạng thái của đường liên kết thành trạng thái Trunk

SW-IT (config-if)# end	Thoát ra khỏi chế độ interface Gig0/1
SW-IT# write	Lưu file cấu hình

❖ SW-NHANSU

SW-NHANSU> en	Chuyển về chế độ cấu hình Privileged
SW-NHANSU# conf t	Chuyển vào chế độ Global Configuration
SW-NHANSU (config)# int range fa0/2-3	Chuyển cấu hình vào chế độ interface Fa0/2 đến Fa0/3
SW-NHANSU (config-if-range)# sw access vlan 20	Gán các port từ port Fa0/2 đến Fa0/3 vào VLAN 20
SW-NHANSU (config-if-range)# exit	Thoát ra chế độ interface Fa0/2 đến Fa0/3
SW-NHANSU (config)# int gig0/1	Chuyển cấu hình vào chế độ interface Gig0/1
SW-NHANSU (config-if)# sw mode trunk	Cho phép interface Gig0/1 hoạt động ở chế độ trunk cố định và đồng thời tự động thương lượng để chuyển đổi trạng thái của đường liên kết thành trạng thái Trunk
SW-NHANSu (config-if)# end	Thoát ra khỏi chế độ interface Gig0/1
SW-NHANSU# write	Lưu file cấu hình

❖ SW-KETOAN

SW-KETOAN> en	Chuyển về chế độ cấu hình Privileged
SW-KETOAN# conf t	Chuyển vào chế độ Global Configuration
SW-KETOAN (config)# int range fa0/1-3	Chuyển cấu hình vào chế độ interface Fa0/1 đến Fa0/3
SW-KETOAN (config-if-range)# sw access vlan 30	Gán các port từ port Fa0/1 đến Fa0/3 vào VLAN 30
SW-KETOAN (config-if-range)# exit	Thoát ra chế độ interface Fa0/1 đến Fa0/3
SW-KETOAN (config)# int gig0/1	Chuyển cấu hình vào chế độ interface Gig0/1

SW-KETOAN (config-if)# sw mode trunk	Cho phép interface Gig0/1 hoạt động ở chế độ trunk cố định và đồng thời tự động thương lượng để chuyển đổi trạng thái của đường liên kết thành trạng thái Trunk
SW-KETOAN (config-if)# end	Thoát ra khỏi chế độ interface Gig0/1
SW-KETOAN# write	Lưu file cấu hình

❖ SW-KINHDOANH

SW-KINHDOANH> en	Chuyển về chế độ cấu hình Privileged
SW-KINHDOANH# conf t	Chuyển vào chế độ Global Configuration
SW-KINHDOANH (config)# int range fa0/1-4	Chuyển cấu hình vào chế độ interface Fa0/1 đến Fa0/4
SW-KINHDOANH (config-if-range)# sw access vlan 40	Gán các port từ port Fa0/1 đến Fa0/4 vào VLAN 40
SW-KINHDOANH (config-if-range)# exit	Thoát ra chế độ interface Fa0/1 đến Fa0/4
SW-KINHDOANH (config)# int gig0/1	Chuyển cấu hình vào chế độ interface Gig0/1
SW-KINHDOANH (config-if)# sw mode trunk	Cho phép interface Gig0/1 hoạt động ở chế độ trunk cố định và đồng thời tự động thương lượng để chuyển đổi trạng thái của đường liên kết thành trạng thái Trunk
SW-KINHDOANH (config-if)# end	Thoát ra khỏi chế độ interface Gig0/1
SW-KINHDOANH# write	Lưu file cấu hình

❖ SW-TANG1

SW-TANG1> en	Chuyển về chế độ cấu hình Privileged
SW-TANG1# conf t	Chuyển vào chế độ Global Configuration
SW-TANG1 (config)# int range fa0/2-3	Chuyển cấu hình vào chế độ interface Fa0/2 đến Fa0/3
SW-TANG1 (config-if-range)# sw access vlan 60	Gán các port từ port Fa0/2 đến Fa0/3 vào VLAN 60
SW-TANG1 (config-if-range)# exit	Thoát ra chế độ interface Fa0/2 đến Fa0/3
SW-TANG1 (config)# int gig0/1	Chuyển cấu hình vào chế độ interface Gig0/1
SW-TANG1 (config-if)# sw mode trunk	Cho phép interface Gig0/1 hoạt động ở chế độ trunk cố định và đồng thời tự động thương lượng để chuyển đổi trạng thái của đường liên kết thành trạng thái Trunk
SW-TANG1 (config-if)# end	Thoát ra khỏi chế độ interface Gig0/1
SW-TANG1# write	Lưu file cấu hình

3. Cấu hình STP (Spanning Tree Protocol)

- Spanning Tree Protocol (STP) là một giao thức ngăn chặn sự lặp vòng, cho phép các bridge truyền thông với nhau để phát hiện vòng lặp vật lý trong mạng. Sau đó giao thức này sẽ định rõ một thuật toán mà bridge có thể tạo ra một cấu trúc mạng logic chứa vòng lặp (loop-free).
- SW-Core

SW-Core>en	Chuyển về chế độ cấu hình Privileged
SW-Core# conf t	Chuyển vào chế độ Global Configuration
SW-Core (config)# spanning-tree mode rapid	Bật giao thức Rapid hoạt động trên switch
SW-Core (config)# spanning-tree vlan 2 root primary	Cấu hình switch trở thành root switch cho VLAN 2
SW-Core (config)# spanning-tree vlan 10 root primary	Cấu hình switch trở thành root switch cho VLAN 10
SW-Core (config)# spanning-tree vlan 20 root primary	Cấu hình switch trở thành root switch cho VLAN 20
SW-Core (config)# spanning-tree vlan 30 root primary	Cấu hình switch trở thành root switch cho VLAN 30
SW-Core (config)# spanning-tree vlan 40 root primary	Cấu hình switch trở thành root switch cho VLAN 40
SW-Core (config)# spanning-tree vlan 50 root primary	Cấu hình switch trở thành root switch cho VLAN 50
SW-Core (config)# spanning-tree vlan 60 root primary	Cấu hình switch trở thành root switch cho VLAN 60
SW-Core (config)# end	Chuyển về chế độ cấu hình Privileged
SW-Core# write	Lưu file cấu hình

Bảng 4: Cấu hình STP

4. Cấu hình địa chỉ IP

❖ Ta sẽ cấu hình địa chỉ IP cho các thiết bị:

- Switch Core: Cấu hình địa chỉ IP giữa switch core với router
- Router
- Router internet: Dùng router giả lập mạng internet, tạo interface loopback là 8.8.8.8, cấu hình IP cho cổng Router nối với Router internet
- Cấu hình địa chỉ IP cho các interfaces VLAN của các Switch Core.
- Đặt IP tĩnh cho Wireless Controller, Server với VLAN tương ứng.
  - Server:
    - Địa chỉ: 10.10.40.100/24
    - Subnet Mask: 255.255.255.0
    - Default Gateway: 10.10.40.1
    - DNS: 8.8.8.8
  - Wireless Controller:
    - Địa chỉ: 10.10.2.100/24
    - Subnet Mask: 255.255.255.0
    - Default- Gateway: 10.10.2.1
    - DNS: 10.10.40.100

❖ SW-Core

SW-Core> en	Chuyển về chế độ cấu hình Privileged
SW-Core# conf t	Chuyển vào chế độ Global Configuration
SW-Core (config)# int vlan 2	Vào chế độ cấu hình của interface VLAN 2
SW-Core (config-if)# ip address 10.10.2.1 255.255.255.0	Gán địa chỉ IP và subnet mask cho interface VLAN 2
SW-Core (config-if)# no shut	Bật interface
SW-Core (config-if)#ex	Thoát ra chế độ interface VLAN 2
SW-Core (config)# int vlan 10	Vào chế độ cấu hình của interface VLAN 10
SW-Core (config-if)# ip address 10.10.10.1 255.255.255.0	Gán địa chỉ IP và subnet mask cho interface VLAN 10
SW-Core (config-if)# no shut	Bật interface
SW-Core (config-if)#ex	Thoát ra chế độ interface VLAN 10
SW-Core (config)# int vlan 20	Vào chế độ cấu hình của interface VLAN 20
SW-Core (config-if)# ip address 10.10.20.1 255.255.255.0	Gán địa chỉ IP và subnet mask cho interface VLAN 20
SW-Core (config-if)# no shut	Bật interface
SW-Core (config-if)#ex	Thoát ra chế độ interface VLAN 20
SW-Core (config)# int vlan 30	Vào chế độ cấu hình của interface VLAN 30
SW-Core (config-if)# ip address 10.10.30.1 255.255.255.0	Gán địa chỉ IP và subnet mask cho interface VLAN 30
SW-Core (config-if)# no shut	Bật interface
SW-Core (config-if)#ex	Thoát ra chế độ interface VLAN 30
SW-Core (config)# int vlan 40	Vào chế độ cấu hình của interface VLAN 40

SW-Core (config-if)# ip address 10.10.40.1 255.255.255.0	Gán địa chỉ IP và subnet mask cho interface VLAN 40
SW-Core (config-if)# no shut	Bật interface
SW-Core (config-if)#ex	Thoát ra chế độ interface VLAN 40
SW-Core (config)# int vlan 50	Vào chế độ cấu hình của interface VLAN 50
SW-Core (config-if)# ip address 10.10.50.1 255.255.255.0	Gán địa chỉ IP và subnet mask cho interface VLAN 50
SW-Core (config-if)# no shut	Bật interface
SW-Core (config-if)#ex	Thoát ra chế độ interface VLAN 50
SW-Core (config)# int vlan 60	Vào chế độ cấu hình của interface VLAN 60
SW-Core (config-if)# ip address 10.10.60.1 255.255.255.0	Gán địa chỉ IP và subnet mask cho interface VLAN 60
SW-Core (config-if)# no shut	Bật interface
SW-Core (config-if)#ex	Thoát ra chế độ interface VLAN 60
SW-Core (config)# int Gig1/0/1	Vào chế độ cấu hình của interface Gig1/0/1
SW-Core (config-if)# no switchport	Bật interface
SW-Core (config-if)# ip address 10.0.1.2 255.255.255.0	Gán địa chỉ IP và subnet mask cho interface Gig1/0/1
SW-Core (config-if)# no shut	Bật interface
SW-Core (config-if)# end	Chuyển về chế độ cấu hình Privileged
SW-Core# write	Lưu file cấu hình

Bảng 5: Cấu hình địa chỉ IP cho switch core

❖ Cấu hình địa chỉ trên Router:

- Cổng Gig0/0 (nối với switch core): 10.0.1.1/24
- Cổng Gig0/1 (nối với internet): 100.0.0.1/24

Router> en	Chuyển về chế độ cấu hình Privileged
Router# conf t	Chuyển vào chế độ Global Configuration
Router (config)# int Gig0/0	Vào chế độ cấu hình của interface Gig0/0
Router (config-if)# ip address 10.0.1.1 255.255.255.0	Gán địa chỉ IP và subnet mask cho interface Gig0/0
Router (config-if)# no shut	Bật interface
Router (config-if)# ex	Thoát ra chế độ interface Gig0/0
Router (config)# int Gig0/1	Vào chế độ cấu hình của interface Gig0/1
Router (config-if)# ip address 100.0.0.1 255.255.255.0	Gán địa chỉ IP và subnet mask cho interface Gig0/1
Router (config-if)# no shut	Bật interface
Router (config)# end	Thoát ra chế độ interface Gig0/1
Router# write	Lưu file cấu hình

Bảng 6: Cấu hình địa chỉ IP cho Router

❖ Cấu hình địa chỉ IP cho cổng Router nối với Router internet, tạo interface loopback là 8.8.8.8

Router> en	Chuyển về chế độ cấu hình Privileged
Router# conf t	Chuyển vào chế độ Global Configuration
Router (config)# hostname INTERNET	Cấu hình tên cho router là INTERNET
INTERNET (config)# int Gig0/0	Vào chế độ cấu hình của interface Gig0/0
INTERNET (config-if)# ip address 100.0.0.1 255.255.255.0	Gán địa chỉ IP và subnet mask cho interface Gig0/0
INTERNET (config-if)# no shut	Bật interface
INTERNET (config-if)# ex	Thoát ra chế độ interface Gig0/0

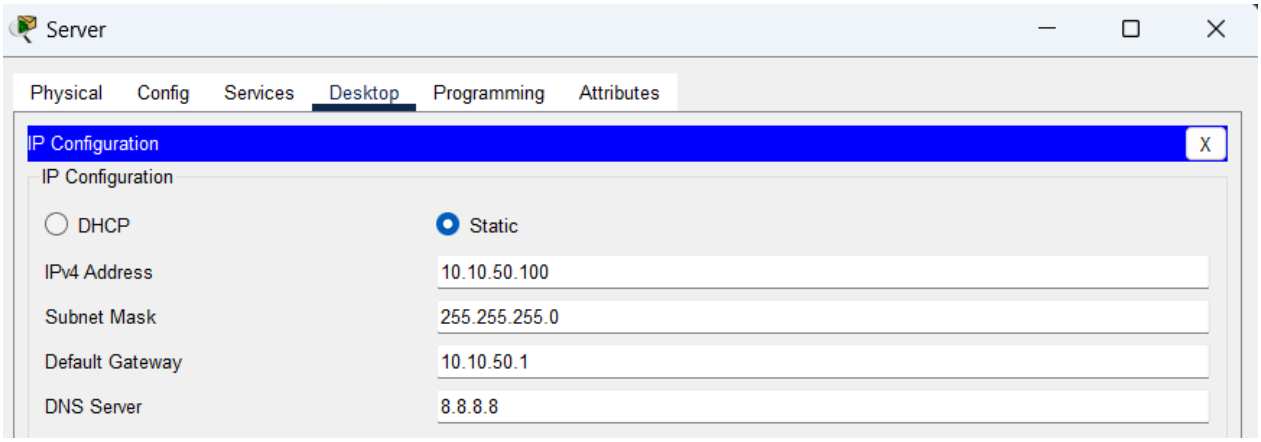
INTERNET (config)# int loopback 0	Tạo một interface ảo tên là loopback 0, và sau đó chuyển vào chế độ cấu hình của interface nay.
INTERNET (config-if)# ip address 8.8.8.8 255.255.255.255	Gán địa chỉ IP và subnet mask cho interface loopback
INTERNET (config-if)# end	Chuyển về chế độ cấu hình Privileged
INTERNET# write	Lưu file cấu hình

Bảng 7: Cấu hình Router giả lập internet

❖ Cấu hình IP tĩnh cho Server và Wireless Controller

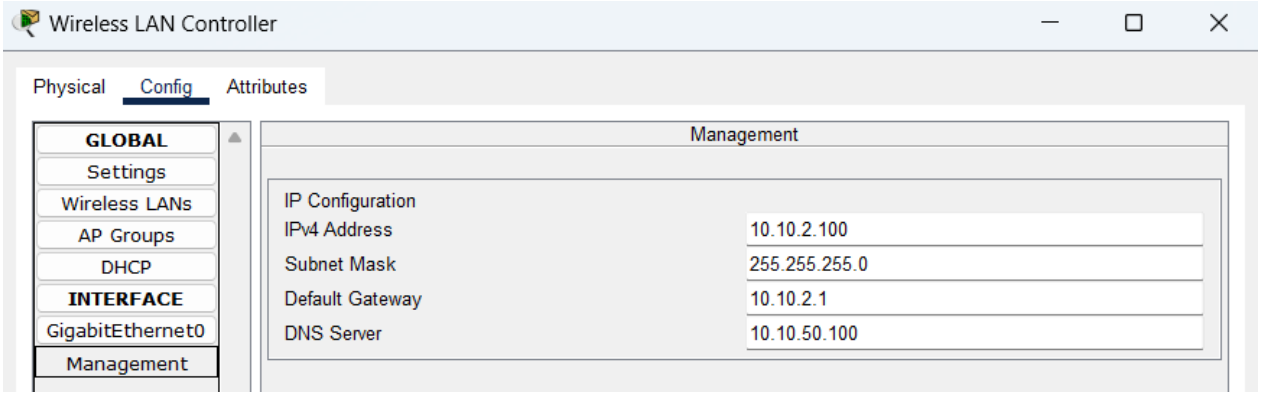
➢ Cấu hình trên Server: Click Server → chọn tab Desktop → Chọn IP Configuration

- Ipv4 address: 10.10.50.100
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.10.50.1
- DNS: 8.8.8.8



Hình 31: Cấu hình địa chỉ IP cho Server

- Cấu hình trên Wireles Controller: Click Wireless Controller → chọn tab Config → Chọn mục Management
  - Ipv4 address: 10.10.2.100
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 10.10.2.1
  - DNS Server: 10.10.50.100



Hình 32: Cấu hình địa chỉ IP cho Wireless Controller

5. Cấu hình EIGRP

❖ EIGRP (Enhanced Interior Gateway Routing Protocol) là một giao thức định tuyến mạnh mẽ và linh hoạt nổi bật với khả năng hội tụ nhanh, tiết kiệm băng thông và hỗ trợ cân bằng tải đa đường. EIGRP giúp duy trì các tuyến đường tối ưu trong mạng nội bộ, đảm bảo mạng hoạt động ổn định và hiệu quả.

❖ Cấu hình giao thức EIGRP trên Router:

Router> en	Chuyển về chế độ cấu hình Privileged
Router# conf t	Chuyển vào chế độ Global Configuration
Router (config)# router eigrp 1	Cho phép router hoạt động với giao thức định tuyến EIGRP AS là 1
Router (config-router)# network 10.0.1.0 0.0.0.255	Chỉ ra những mạng sẽ được quảng bá bởi EIGRP
Router (config-router)# end	Chuyển về chế độ cấu hình Privileged
Router# write	Lưu file cấu hình

Bảng 8: Cấu hình giao thức EIGRP trên Router

6. Cấu hình Default Route

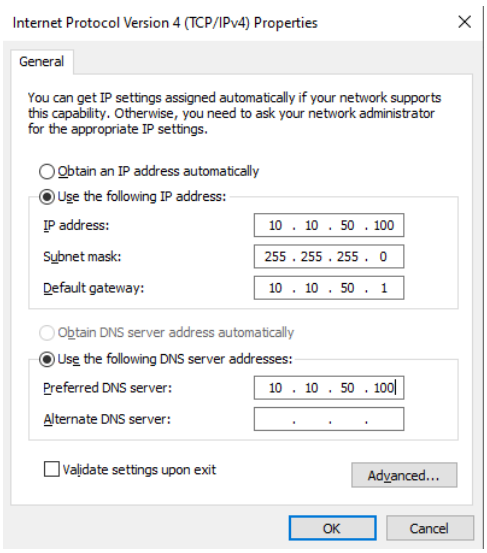
- Cấu hình default route trên router là quyết định định tuyến mặc định, đó là khi router không biết địa chỉ IP cụ thể của đích đến trong bảng định tuyến của mình, nó sẽ chuyển gói tin đến một định tuyến mặc định đã được xác định trước, cho phép router thoát ra khỏi mạng nội bộ và chuyển tiếp gói tin đến mạng bên ngoài, chẳng hạn Internet hoặc một mạng WAN khác.
- Router

Router>en	Chuyển về chế độ cấu hình Privileged
Router# conf t	Chuyển vào chế độ Global Configuration
Router (config)# ip route 0.0.0.0 0.0.0.0 Gig0/1	Tạo 1 default Route ở Router
Router (config)# end	Chuyển về chế độ cấu hình Privileged
Router# write	Lưu file cấu hình

Bảng 9: Cấu hình Default Route

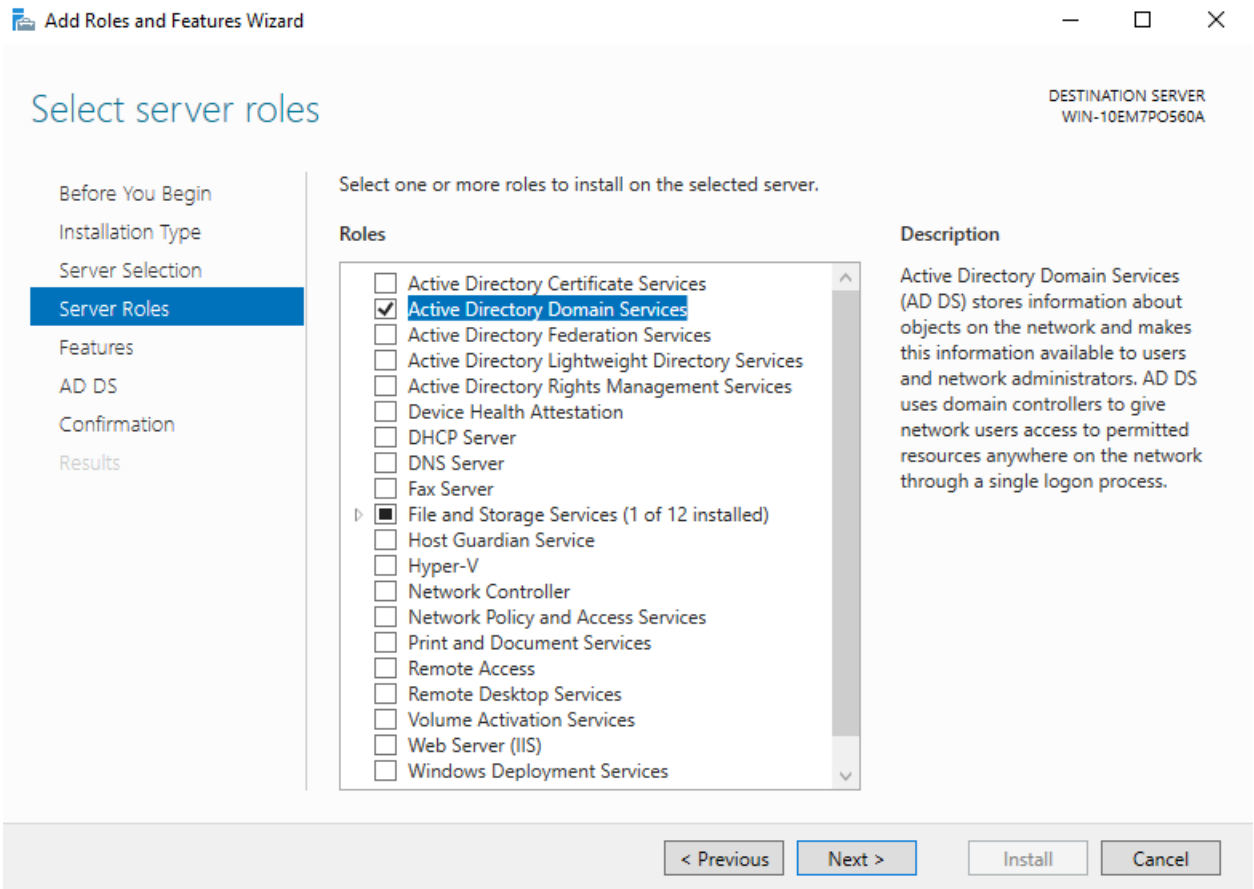
7. Triển khai dịch vụ Domain Controller

- Dịch vụ Domain Controller (DC) là một phần quan trọng của hệ thống Active Directory trong môi trường Windows Server, đóng vai trò quan trọng trong việc quản lý, bảo mật và phân phối các tài nguyên và dịch vụ trong một mạng Windows domain. Ta sẽ sử dụng máy chủ Server để lên Domain Controller, các client trong hệ thống sẽ join client vào Domain
- Đầu tiên ta đặt IP tĩnh cho Server: 10.10.50.100



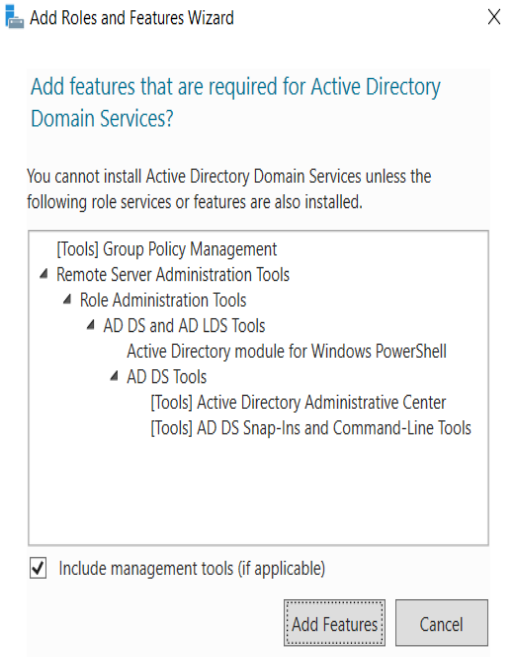
Hình 33: Đặt IP tĩnh cho Server

❖ Kế đến vào Server Manager → chọn Add Roles And Features → chọn dịch vụ Active Directory Domain Services



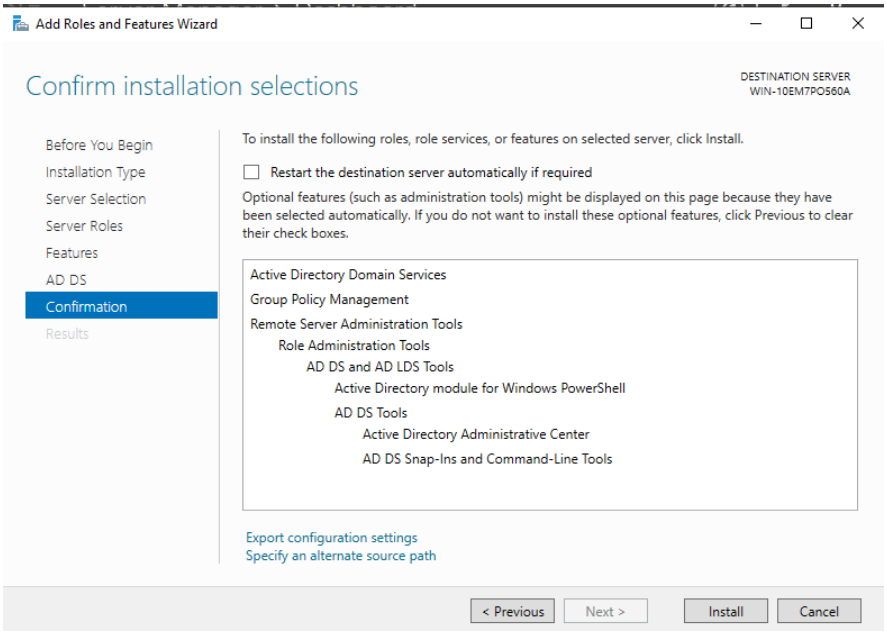
Hình 34: Add Roles And Features

❖ Tiếp theo chọn Add Features



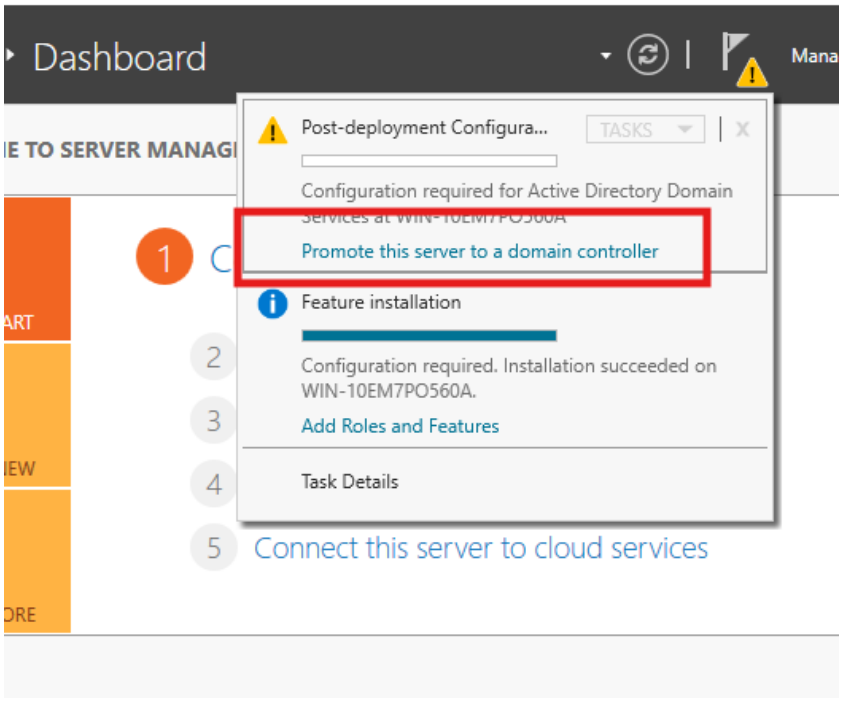
Hình 35: Add Features

❖ Ấn Next tới khi thấy Intall thì nhấn vào

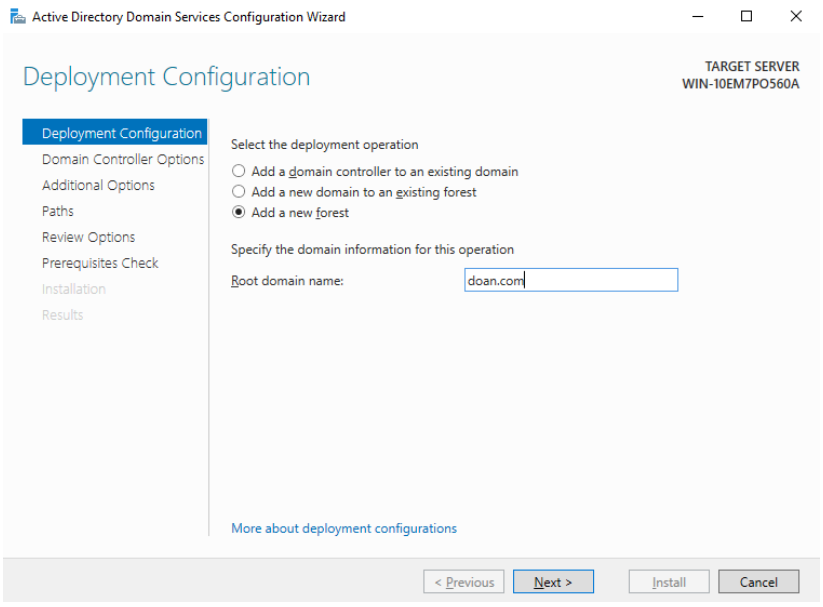


Hình 36: Cài đặt dịch vụ Domain Controller

❖ Sau khi cài đặt xong, ta chọn vào mục Notifications, chọn vào "Promote this server to a domain controller" để thiết lập

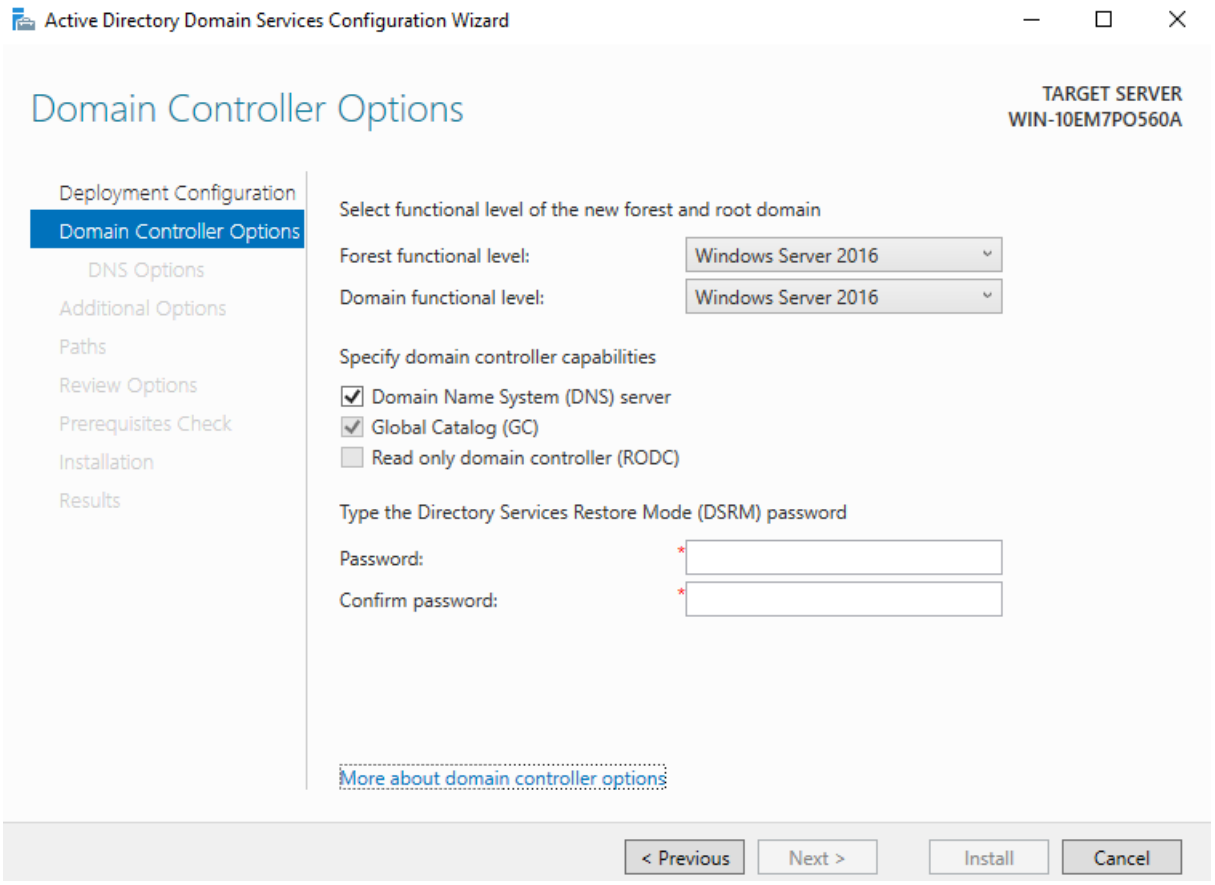


❖ Ta chọn vào "Add a new forest", ở mục "Root domain name" ta đặt tên miền cho domain là: doan.com



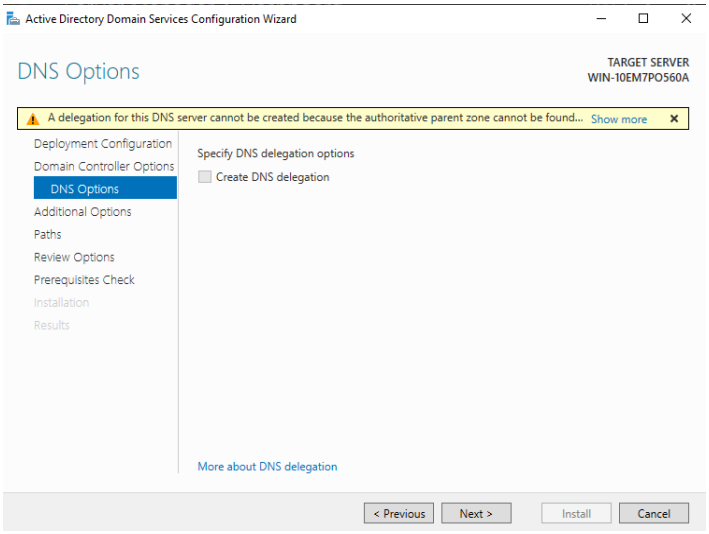
Hình 37: Tạo Domain

❖ Nhấn next, đến bước tiếp theo ta đặt password restore cho Domain (password phải đủ độ phức tạp bao gồm: chữ hoa, chữ thường, kí tự đặc biệt, số, độ dài kí tự từ 8 kí tự trở lên)

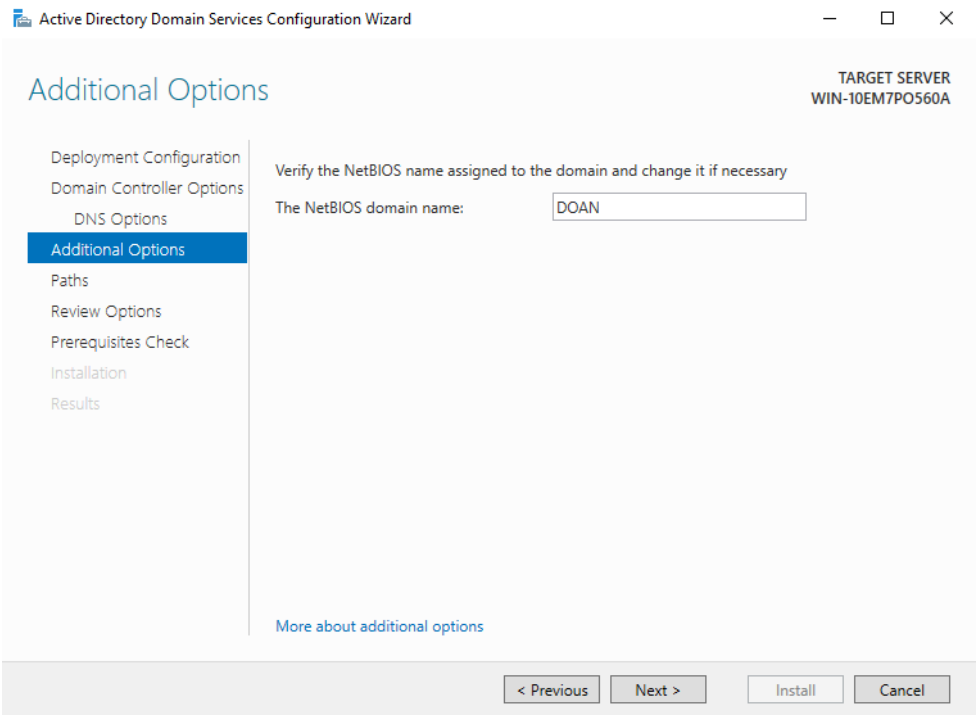


Hình 38: Đặt Password restore cho Domain

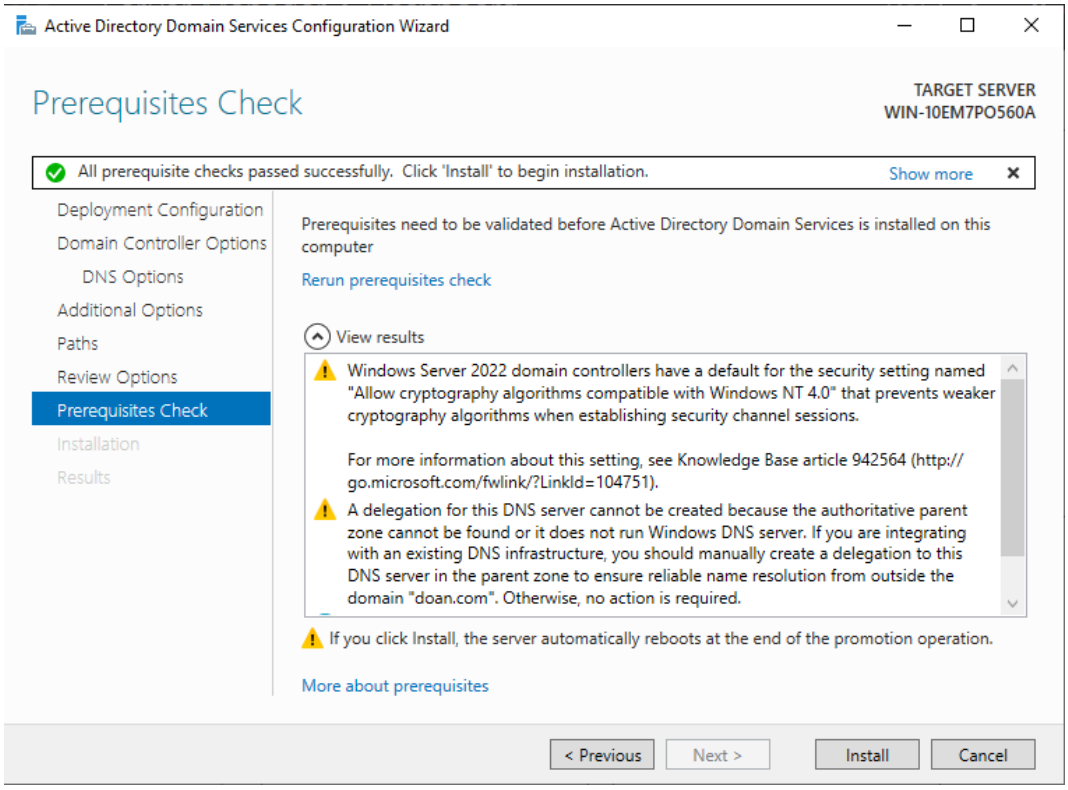
❖ Nhấn next ở bước tiếp theo



❖ The NetBIOS domain name đã được tạo ở bước tiếp theo với tên: DOAN



❖ Tiếp tục nhấn next ở các bước tiếp theo đến khi thấy nút Install thì nhấn vào để cài đặt



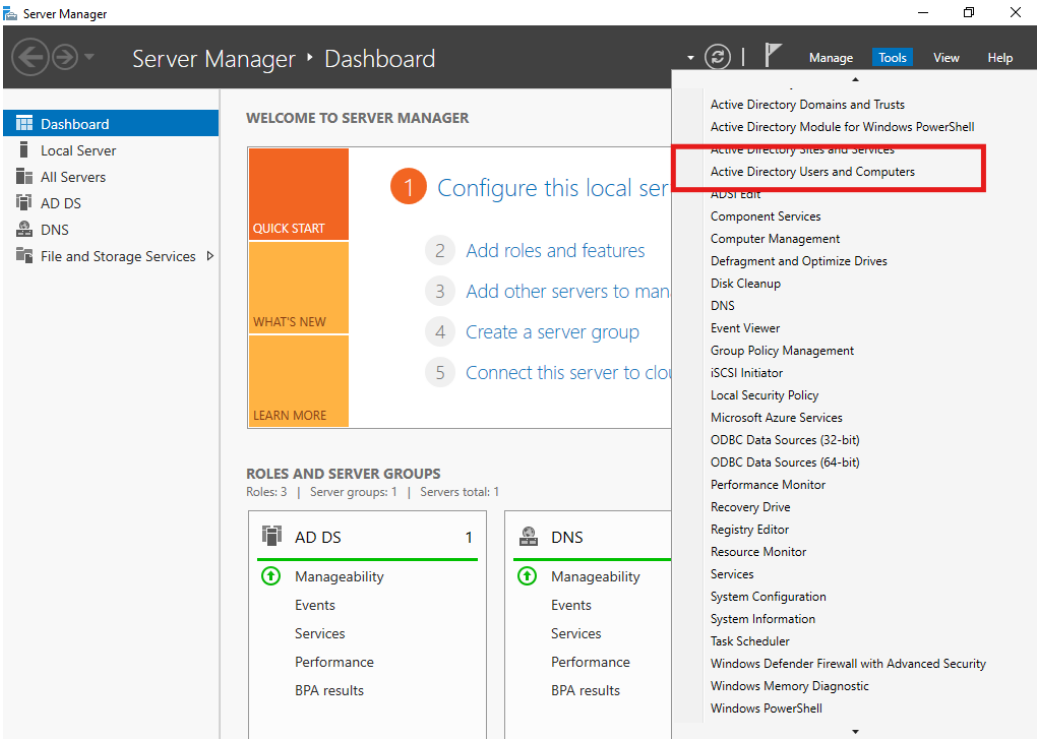
Hình 39: Cài đặt Domain Controller

8. Triển khai tạo User quản lý người dùng

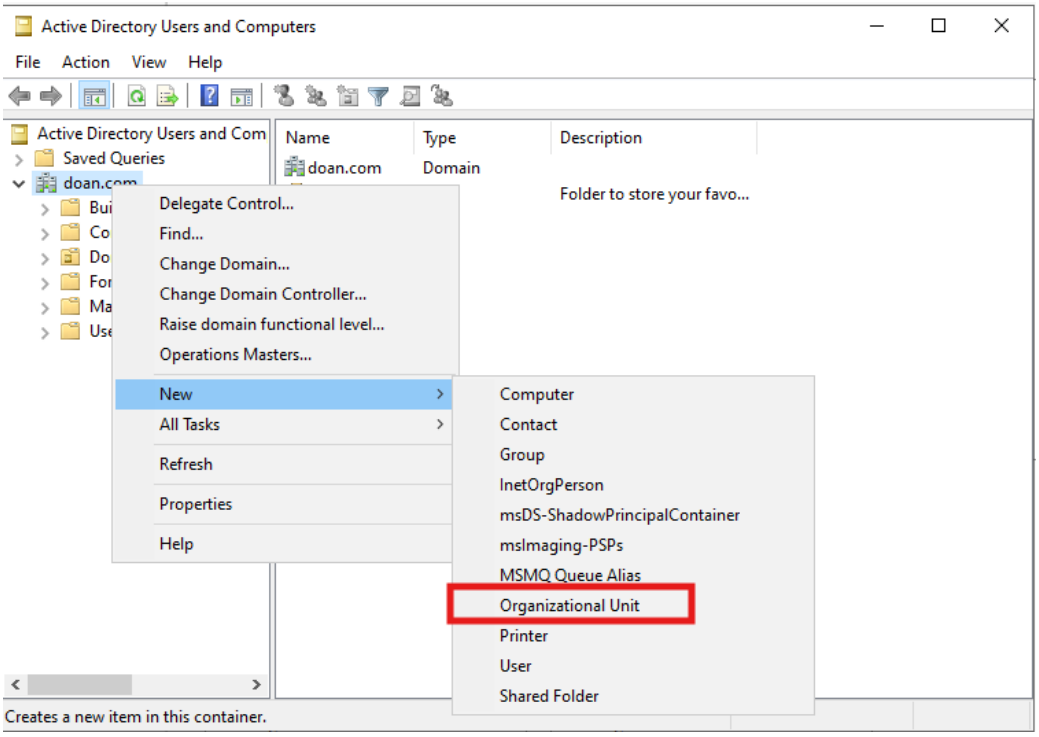
❖ Việc tạo User và quản lý người dùng trong Server là một phần quan trọng của việc duy trì và bảo vệ hệ thống mạng. Điều này giúp đảm bảo rằng người dùng có quyền truy cập phù hợp và duy trì tính bảo mật và hiệu suất của hệ thống.

- ➢ Trước tiên tạo OU (Organizational Unit) để chứa các group user
- ➢ Sau đó ta sẽ tạo các group user tương ứng với các phòng ban.
- ➢ Sau đó ta sẽ tạo các user tương ứng trong các group user.

❖ Ở mục Tools trong Server Manager, ta chọn vào Active Directory User and Computers

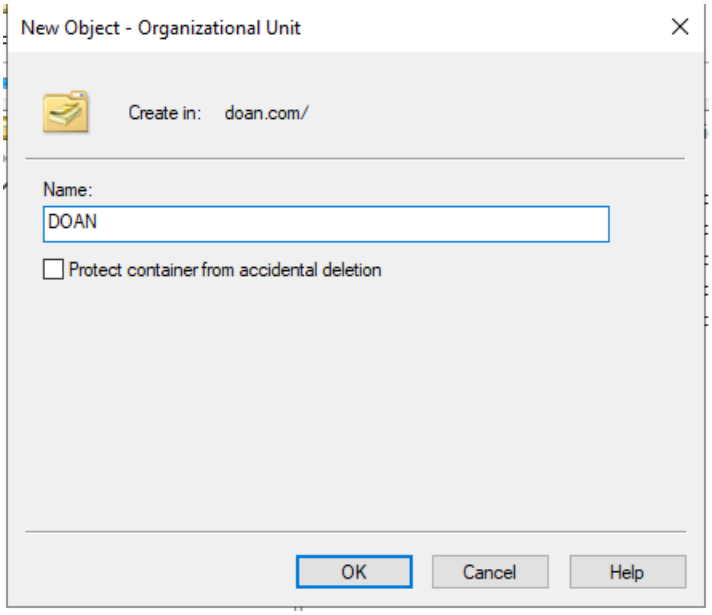


❖ Tiếp theo ta nhấp chuột phải chọn vào domain → New → Organizational Unit

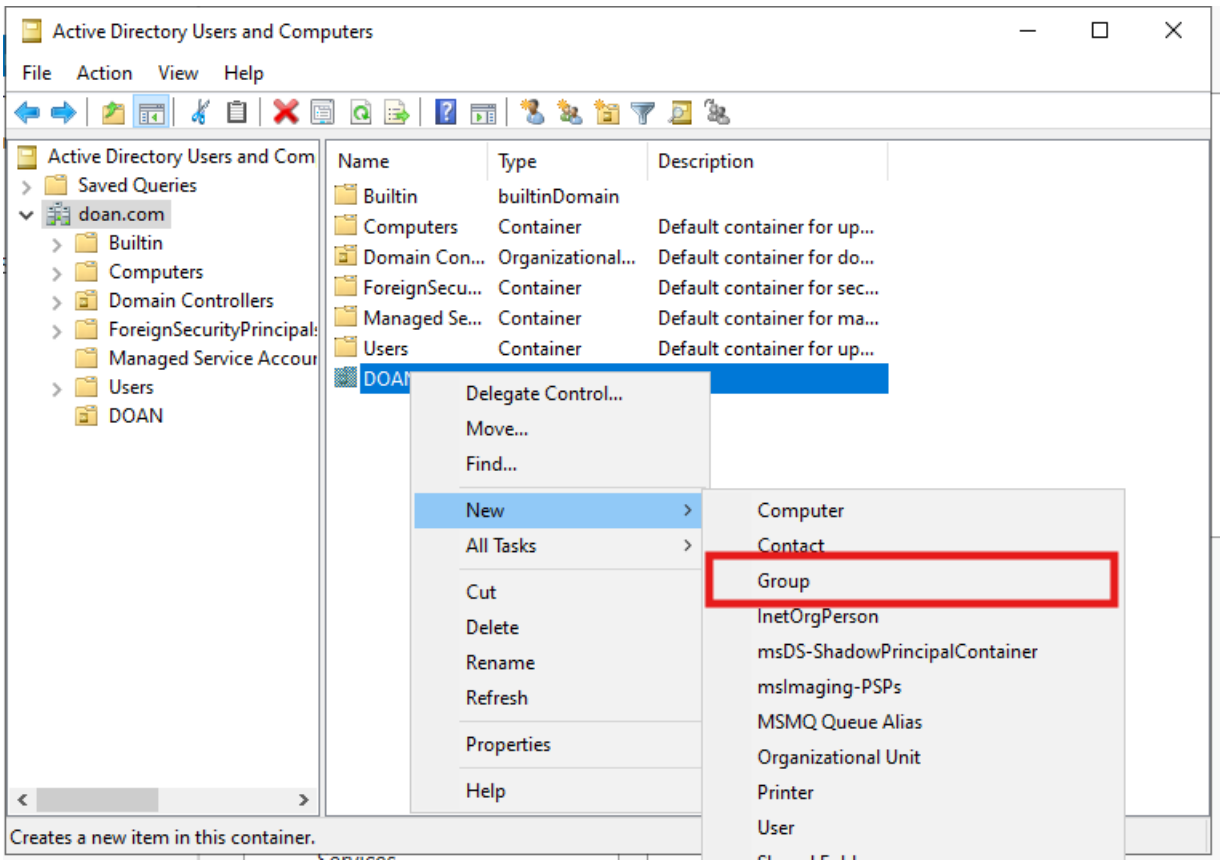


Hình 40: Tạo OU

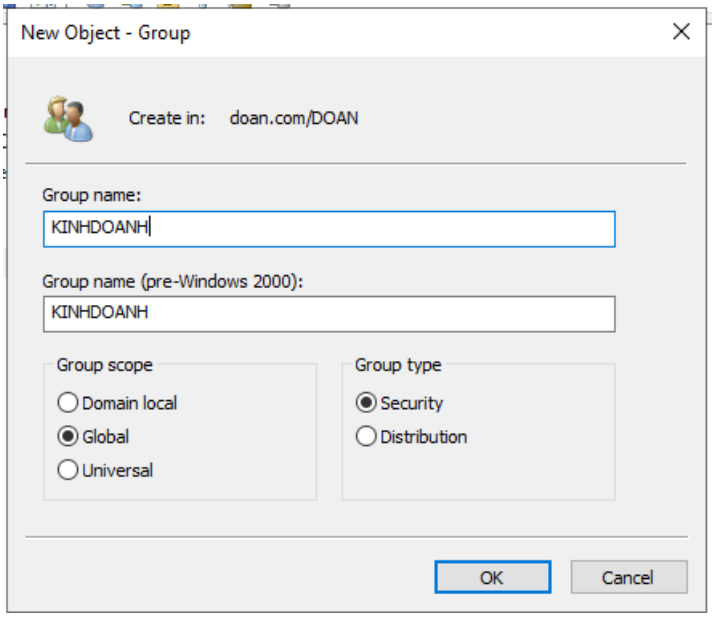
❖ Tạo OU có tên: DOAN



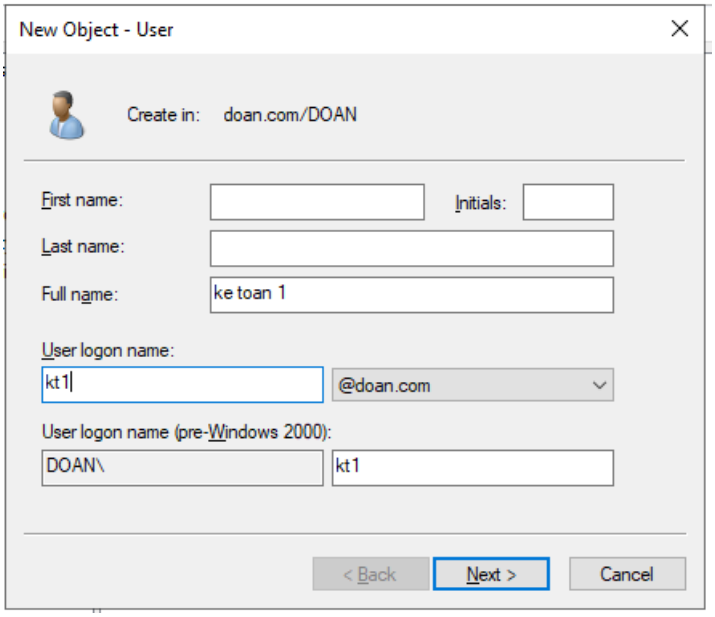
❖ Tiếp theo ta sẽ tạo Group: click phải chuột vào OU vừa tạo → new → group.



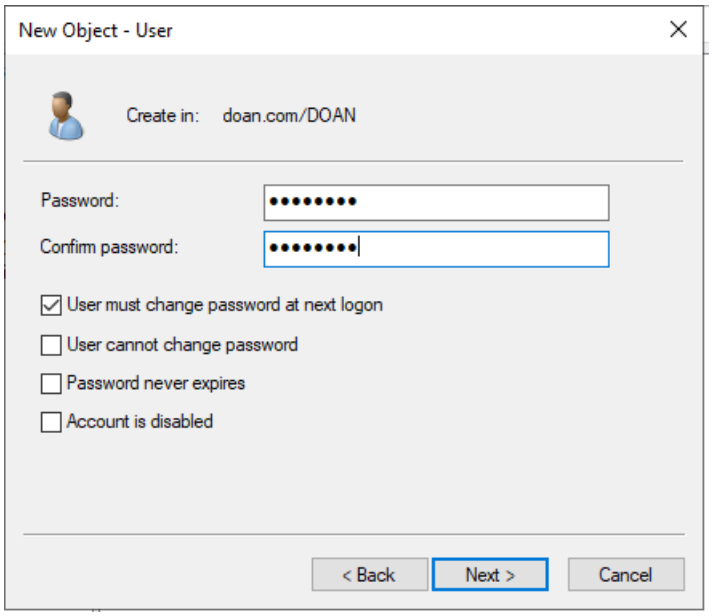
❖ Ta sẽ tạo các group tương ứng với các phòng ban của công ty, bao gồm: IT, KETOAN, KINHDOANH, NHANSU, TANG1



❖ Tạo và thêm user vào group: Click phải trên màn hình trắng phía tay phải → chọn new → user. Ở đây ta sẽ tạo các user liên quan đến các phòng ban



❖ Ở bước này ta sẽ tạo mật khẩu cho user(đủ độ phức tạp), đồng thời tích chọn yêu cầu người dùng đổi mật khẩu trong lần đăng nhập kế tiếp

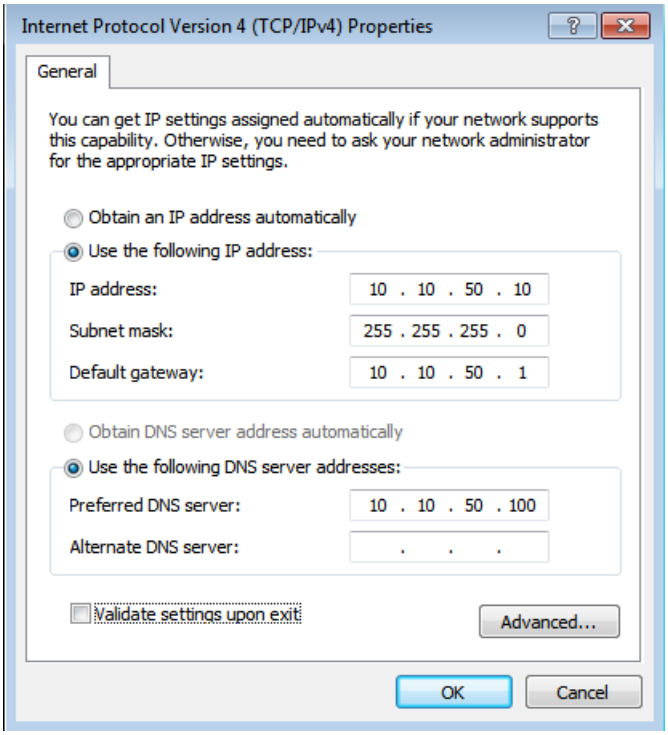


9. Join Client vào Domain và đăng nhập bằng user đã tạo

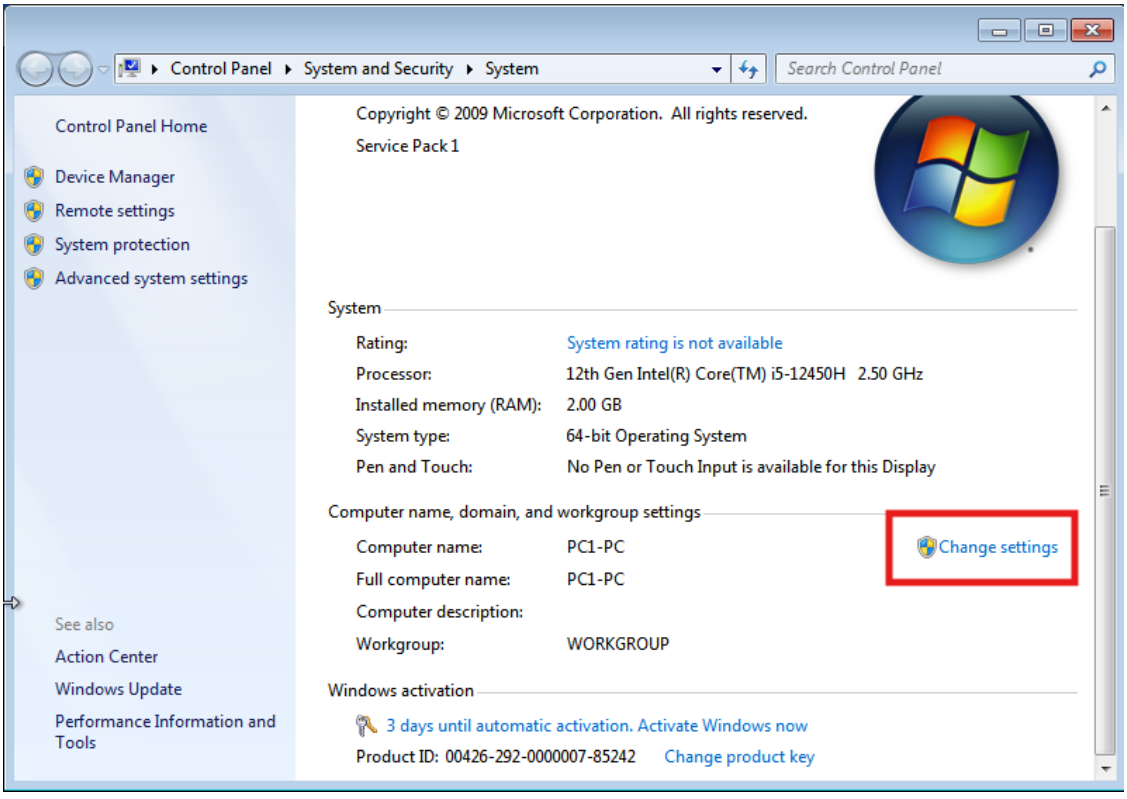
❖ Quy trình join client vào Domain:

- ➢ Đặt IP tĩnh cùng network với DC server
- ➢ Change Name Computer (đổi Workgroup sang Domain).
- ➢ Nhập user/password xác thực.
- ➢ Đăng nhập bằng user/password do DC tạo ra.

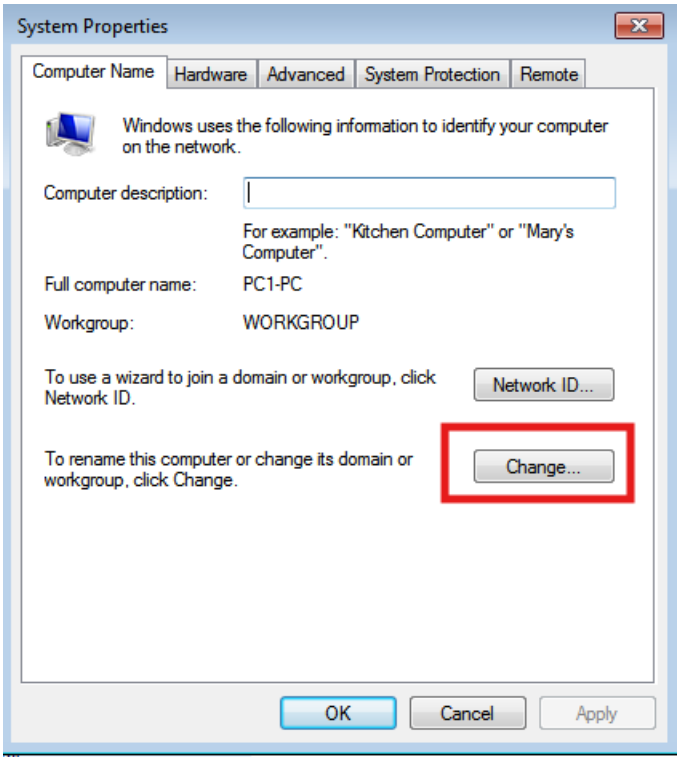
❖ Đầu tiên ta sẽ đặt IP tĩnh cùng network với DC

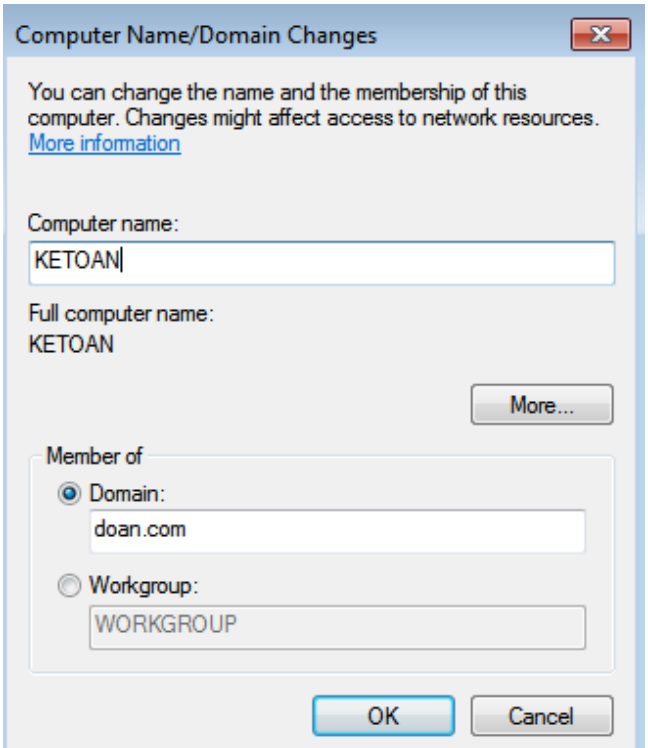


❖ Phải chuột vào biểu tượng computer ở màn hình desktop → Properties → kéo xuống dưới và chọn Change settings

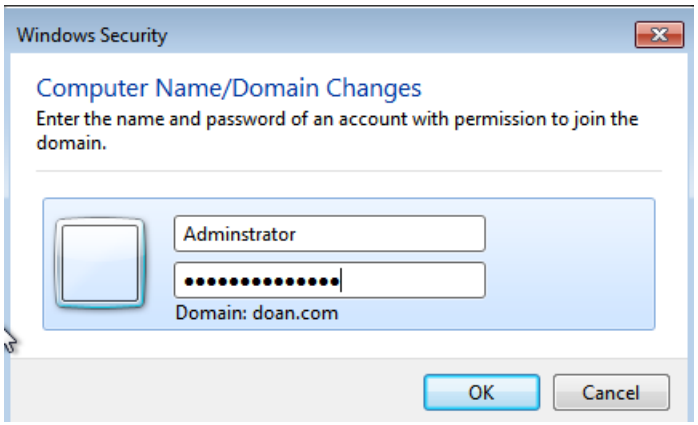


❖ Tiếp theo ta sẽ chọn vào Change…, khi vào cửa sổ computer/Domain changes, ta chuyển Member of thành Domain, và điền domain của server: doan.com → OK

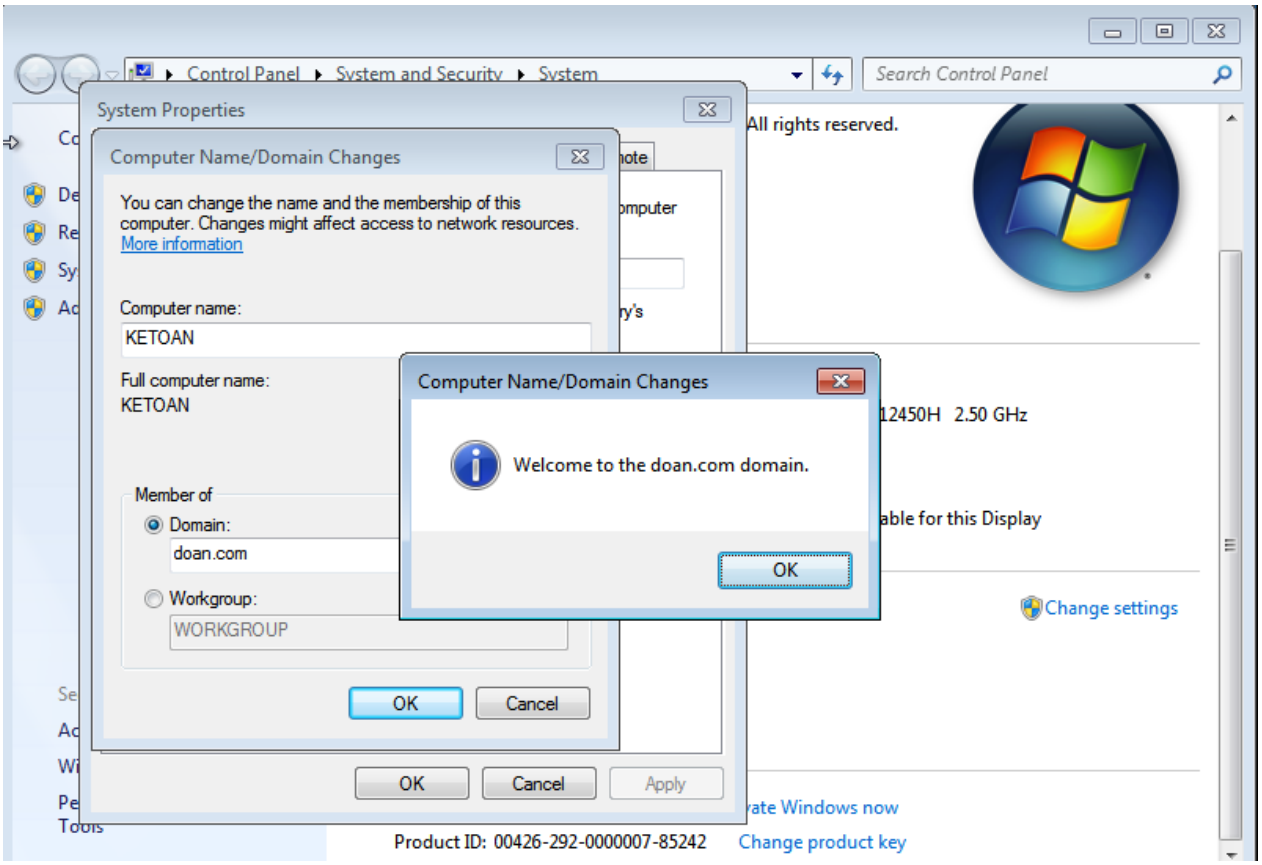




❖ Đăng nhập bằng quyền Administrator của Server:



❖ Join thành công vào Domain doan.com

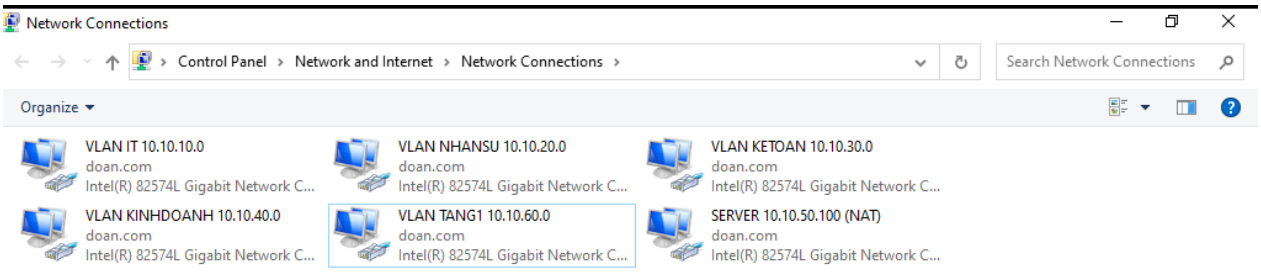


Hình 41: Join Client vào Domain thành công

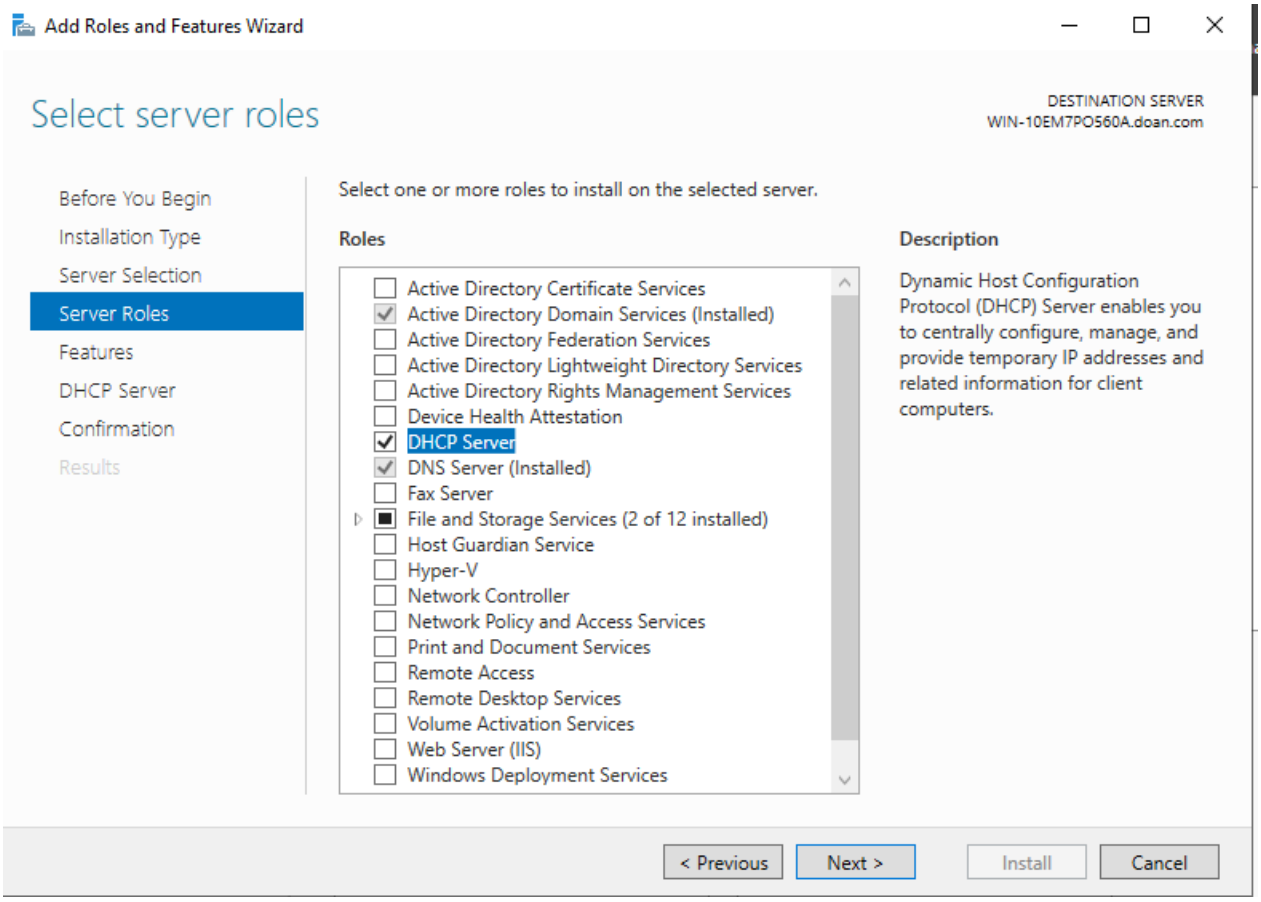
10. Cấu hình DHCP

❖ Ta sẽ cấu hình DHCP ở Server để cấp IP động cho các Client, IP của các Client sẽ tương ứng với VLAN của mỗi phòng ban.

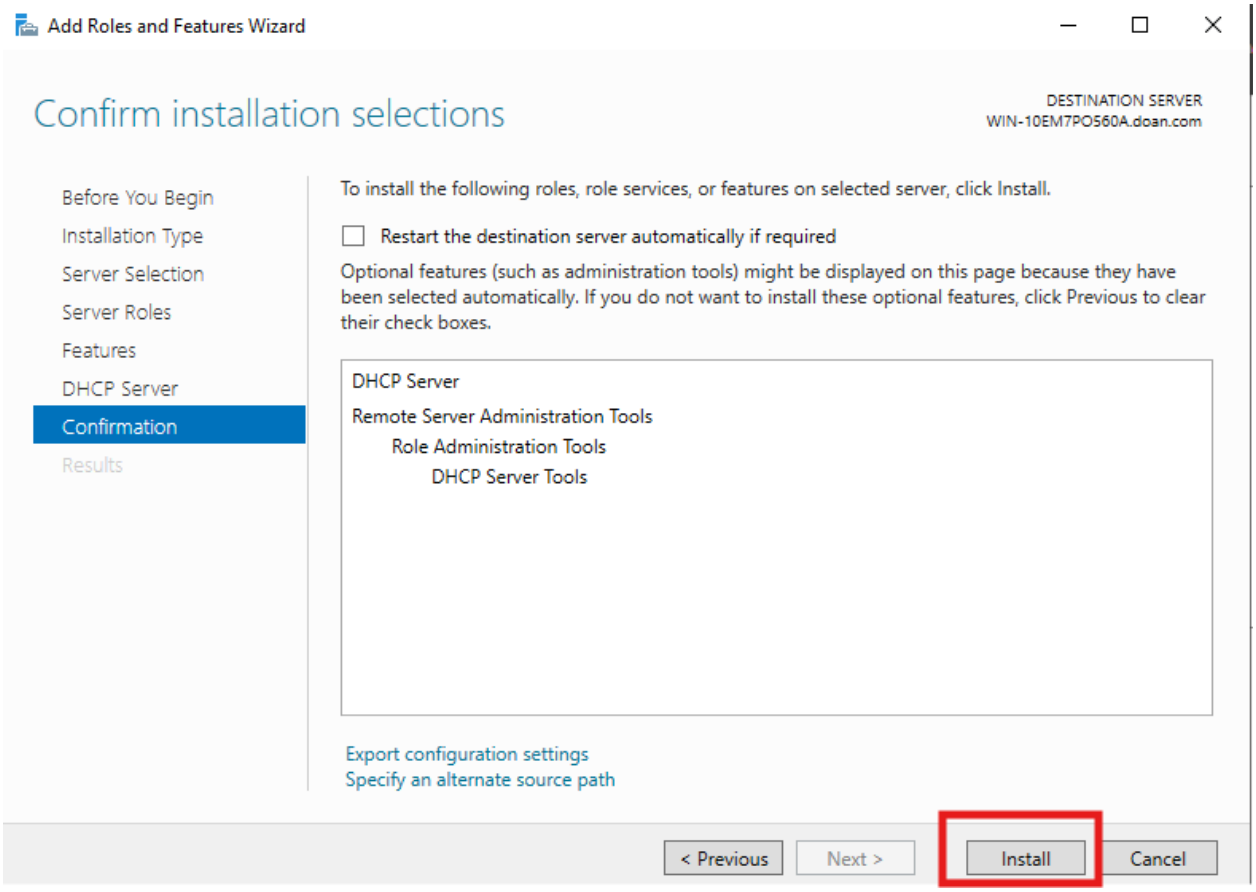
➢ Đầu tiên ta sẽ thêm card mạng tương ứng với các VLAN, đồng thời thay đổi card mạng của các client phòng ban ứng với card mạng có trên Server tương ứng với các VLAN.



➢ Vào Server Manager → chọn Add Roles And Features → chọn dịch vụ DHCP Server và nhấn next.

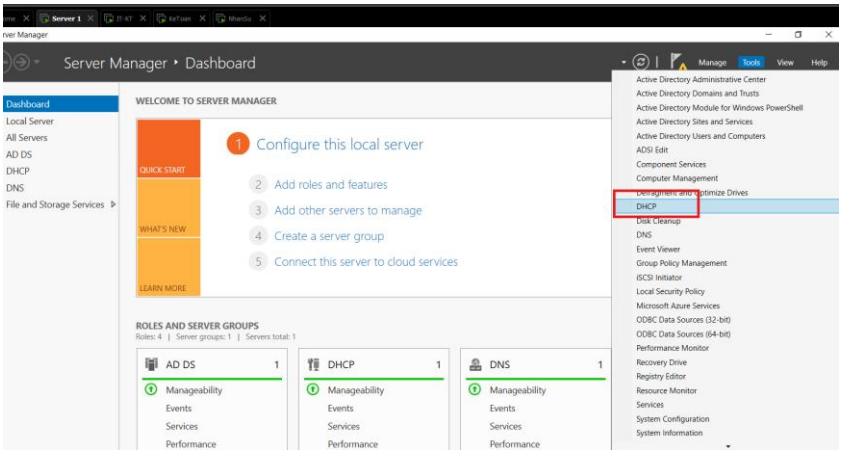


➢ Tiếp tục nhấn next đến khi thấy Install thì nhấn để cài đặt

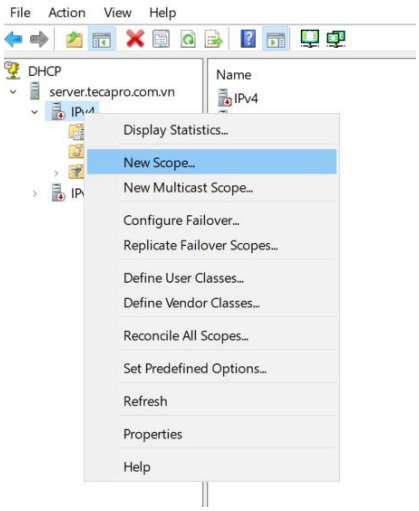


Hình 42: Cài đặt dịch vụ DHCP cho Server

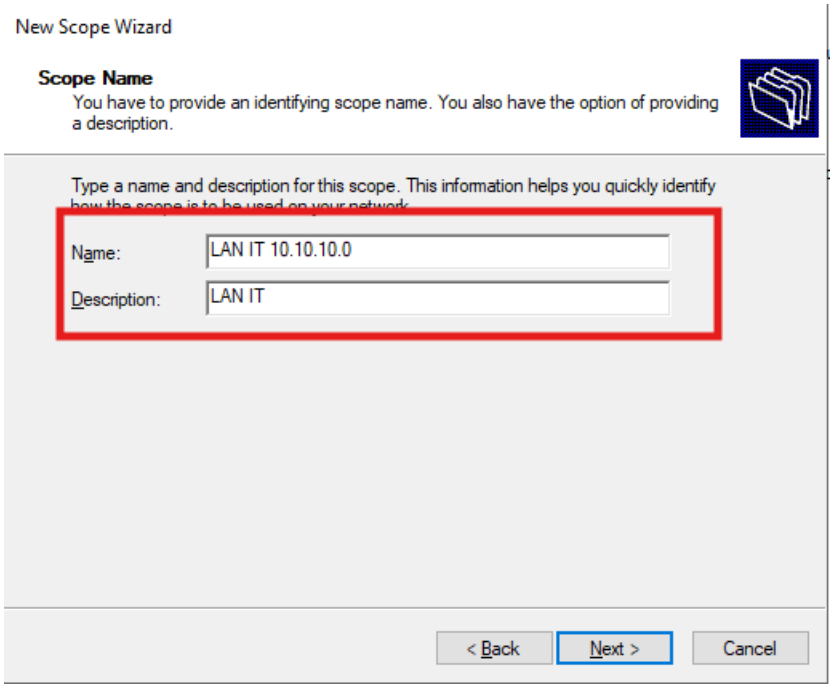
➢ Sau khi cài đặt xong, ở mục Tools trong Server Manager, ta chọn vào DHCP



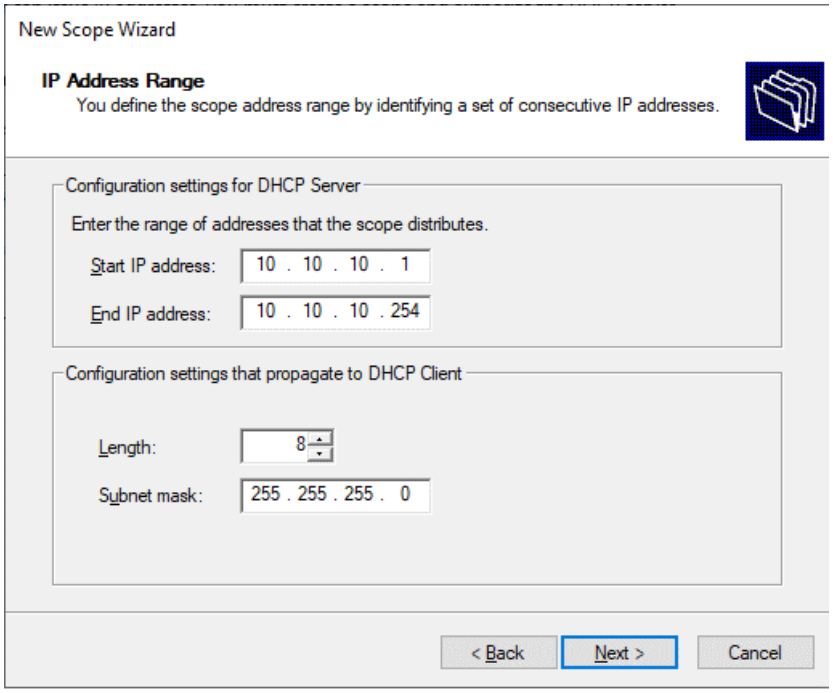
- Tiếp theo ta sẽ tạo New Scope



- Tạo Scope name

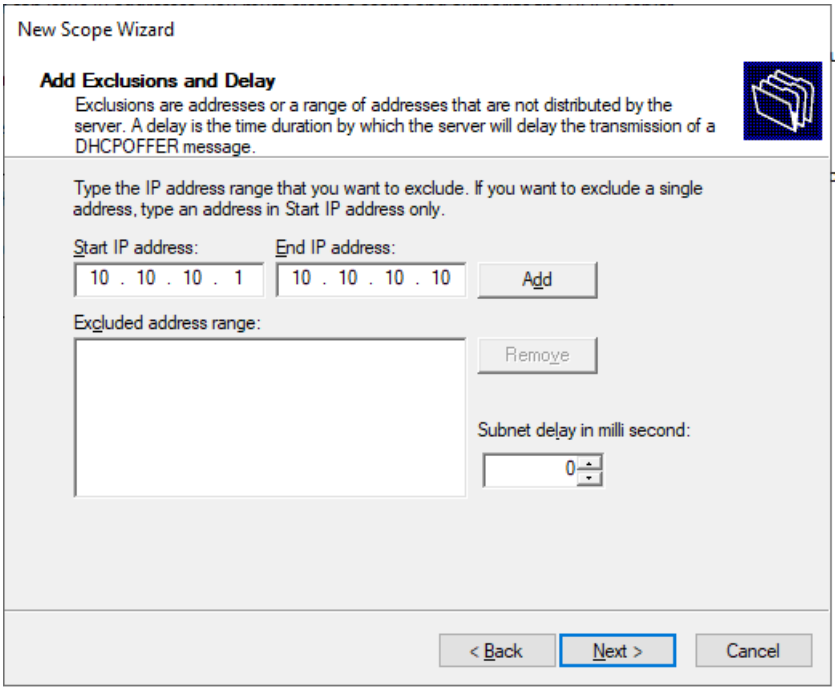


- Tạo dải IP bắt đầu và IP kết thúc được cấp

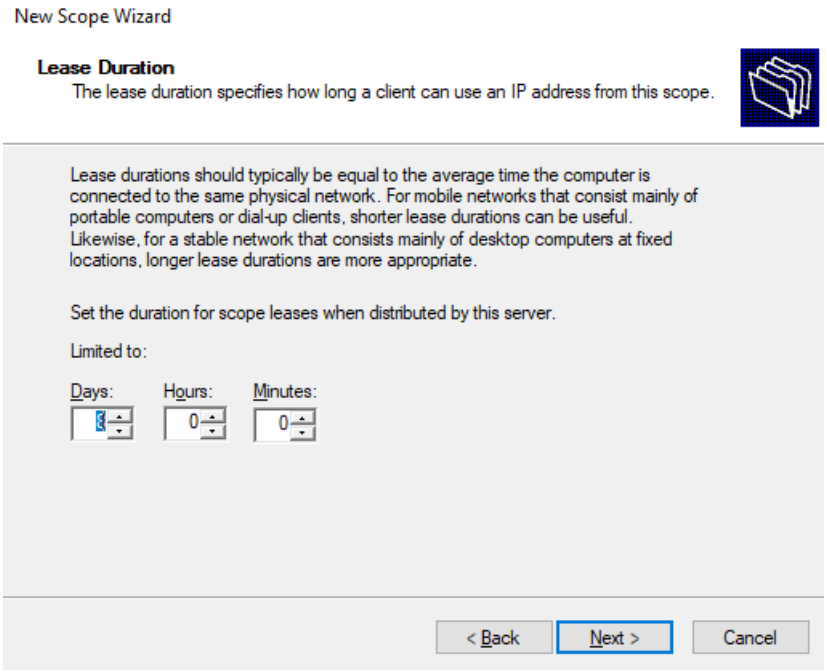


Hình 43: Tạo IP cấp DHCP

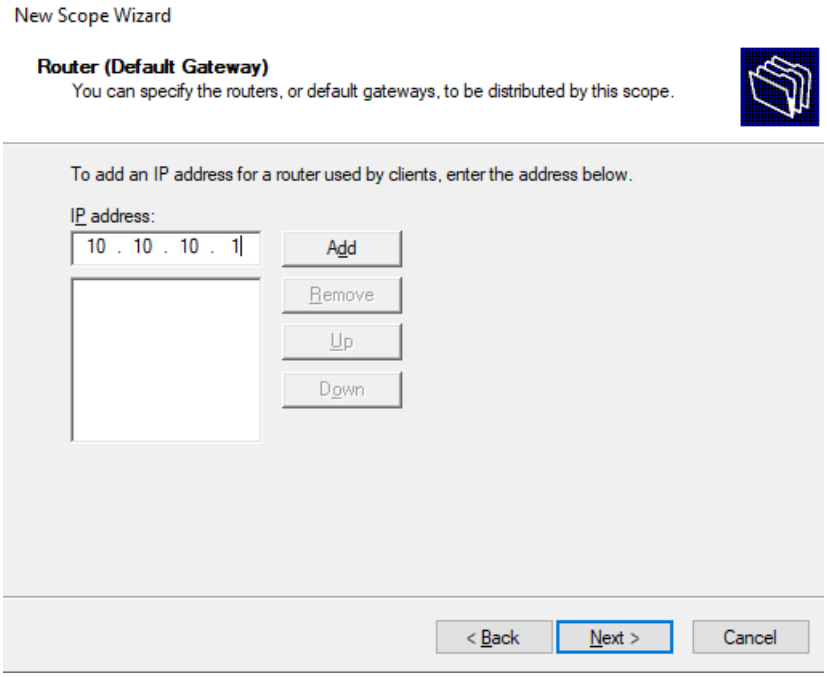
- Tạo dải IP không được phép cấp cho host



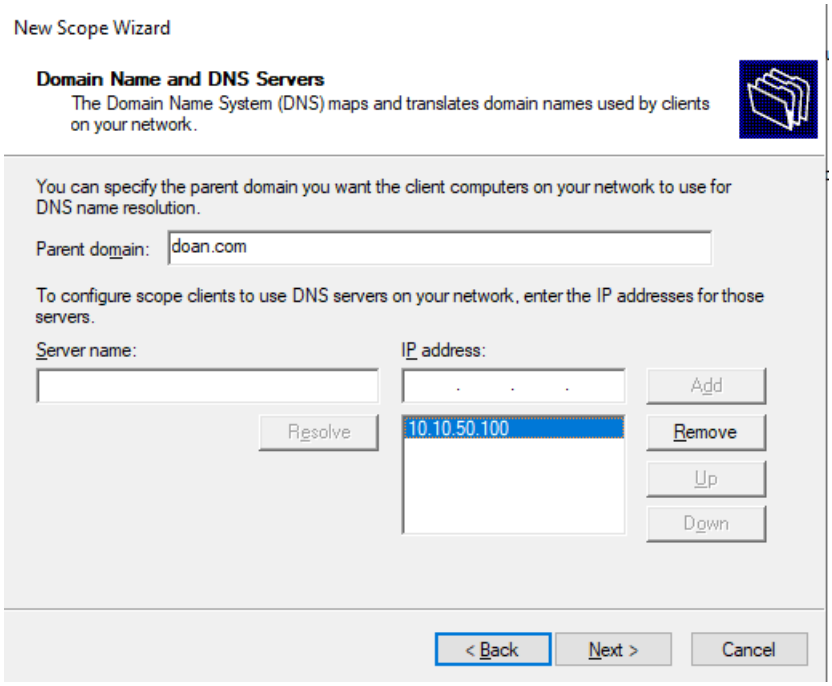
- Thời gian cấp phát lại IP mới



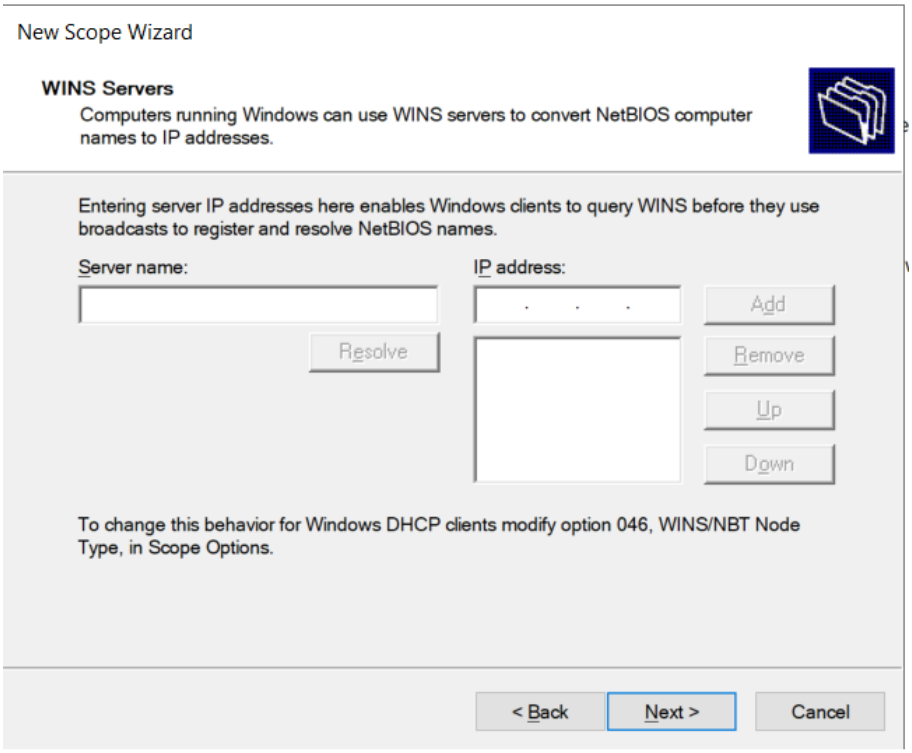
- Tạo default getway

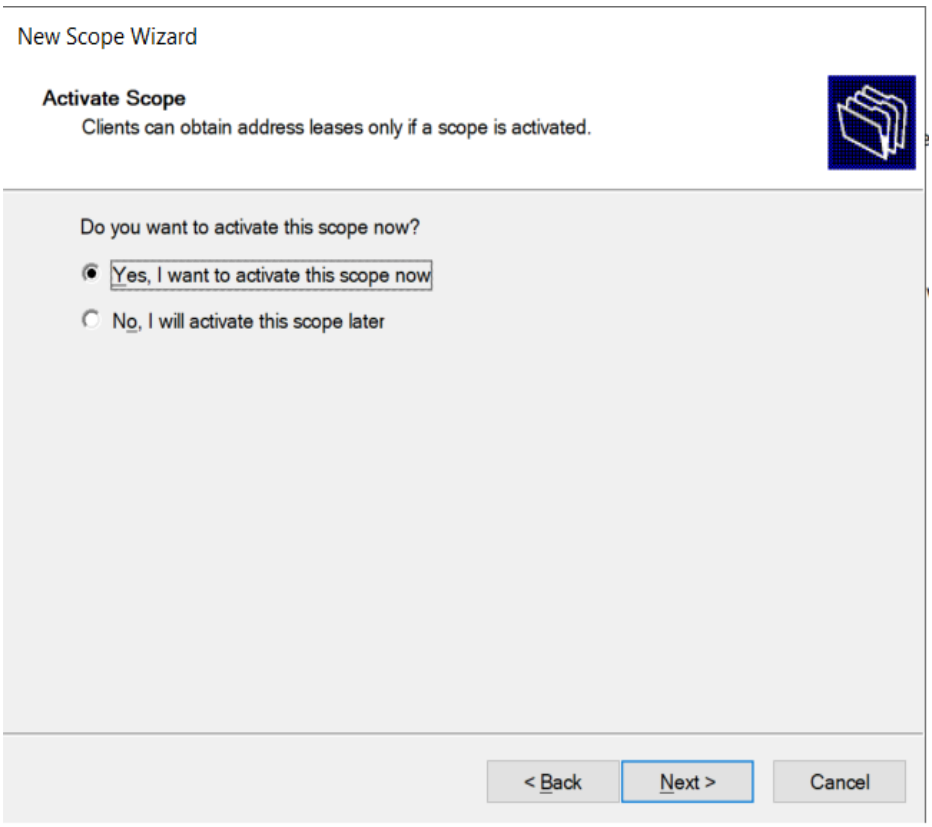


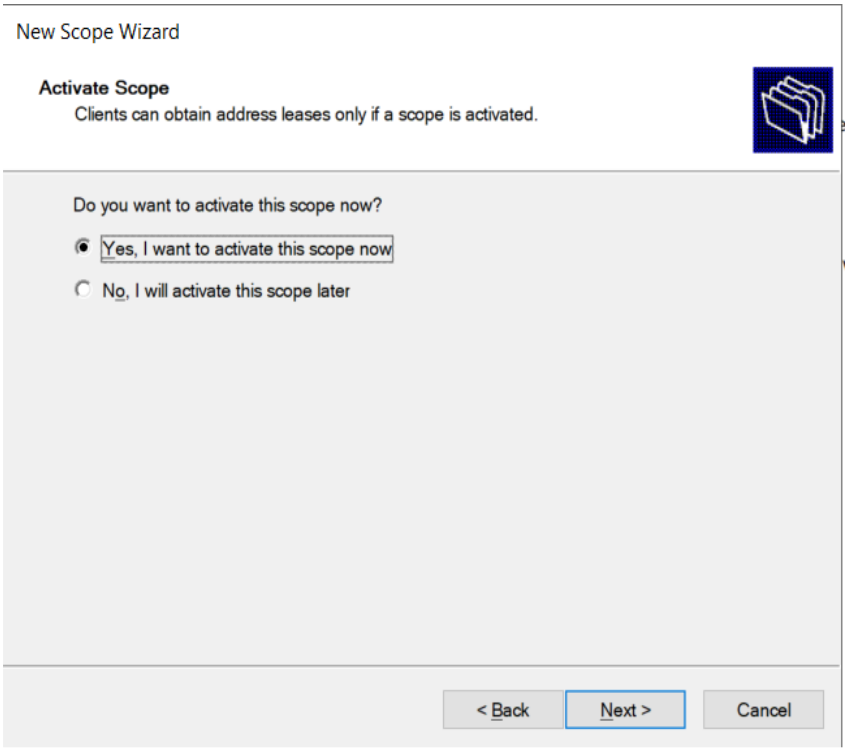
- Thêm Domain và DNS Server:



- Ở đây nhấn next vì không cấu hình DHCP Relay agent



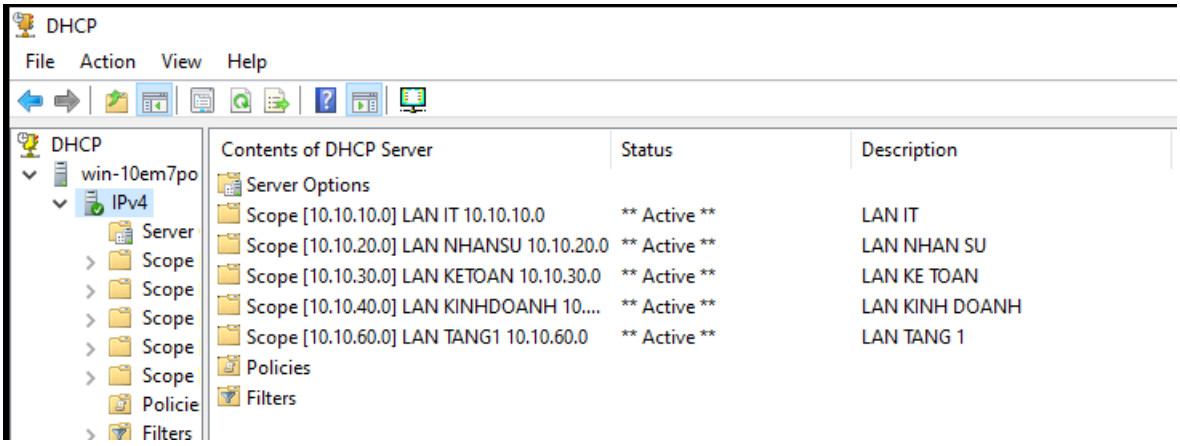

New Scope Wizard
Activate Scope
Clients can obtain address leases only if a scope is activated.
Do you want to activate this scope now?
Yes, I want to activate this scope now
No, I will activate this scope later
< Back
Next >
Cancel


New Scope Wizard
Activate Scope
Clients can obtain address leases only if a scope is activated.
Do you want to activate this scope now?
Yes, I want to activate this scope now
No, I will activate this scope later
< Back
Next >
Cancel

➢ Dãy Scope sau khi tạo xong

Start IP Address	End IP Address	Description
10.10.10.1	10.10.10.254	Address range for distribution
10.10.10.1	10.10.10.10	IP Addresses excluded from distribution

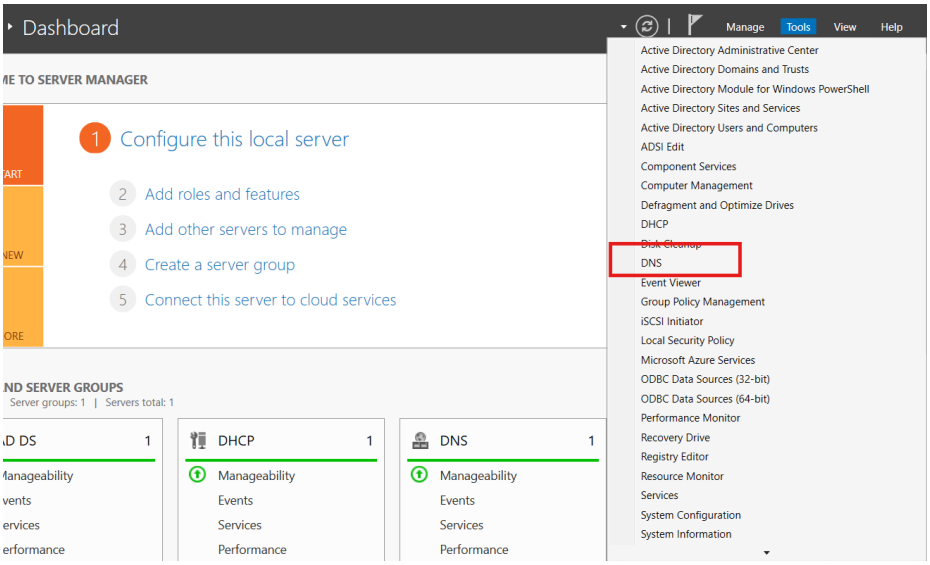
❖ Tương tự với các dãy mạng khác, sau khi tạo tương ứng với VLAN ta được



11. Cấu hình DNS Server

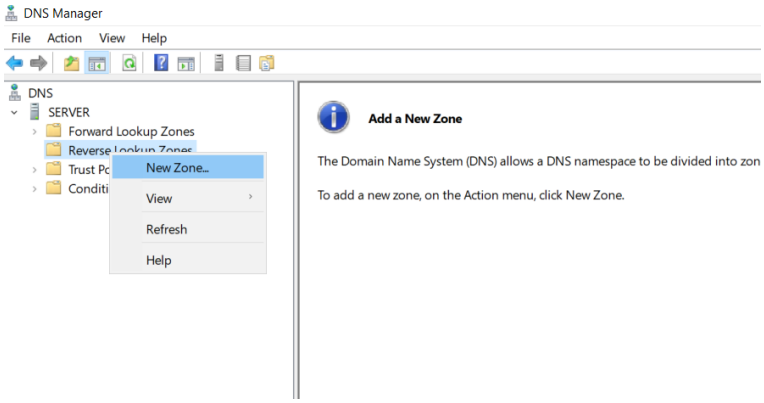
❖ Ở đây ta sẽ cấu hình Reverse Lookup Zones, nghĩa là phân giả ngược tên miền thành địa chỉ IP, vì khi cấu hình Domain hệ thống đã lấy tên Domain để cấu hình DNS thuận từ địa chỉ IP thành tên miền, nên ta chỉ tạo Host ở Forward

➢ Trên Server: cài đặt dịch vụ DNS

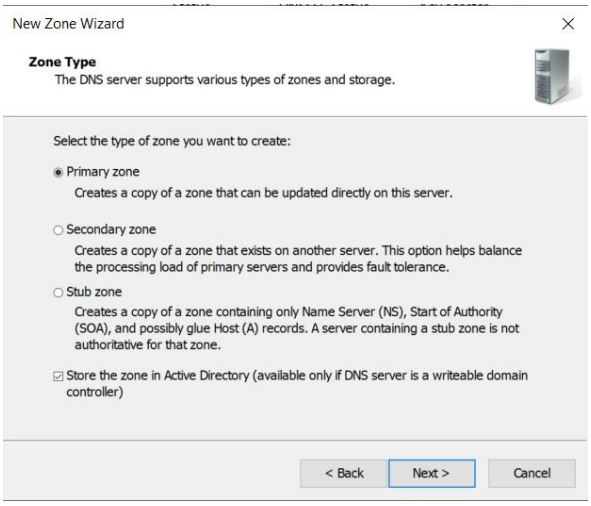


Hình 44: Tạo DNS

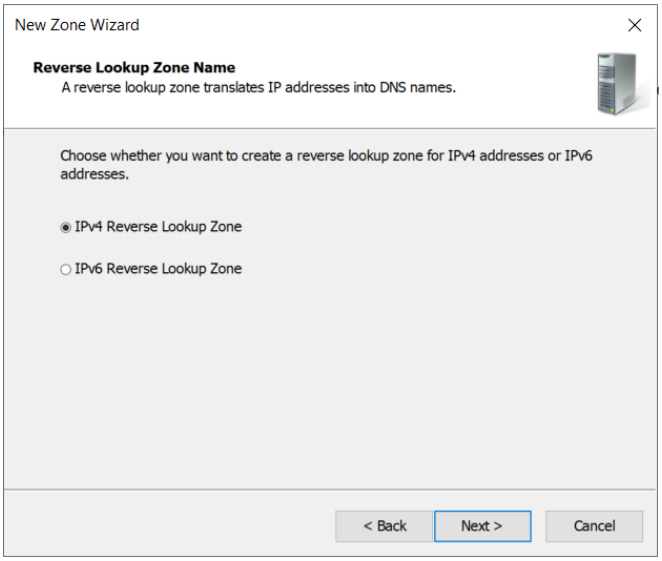
➢ Tạo vùng zone mới cho DC để phân giải từ IP sang tên miền, ta vào Tools → DNS → Reverse Lookup Zones → New Zone



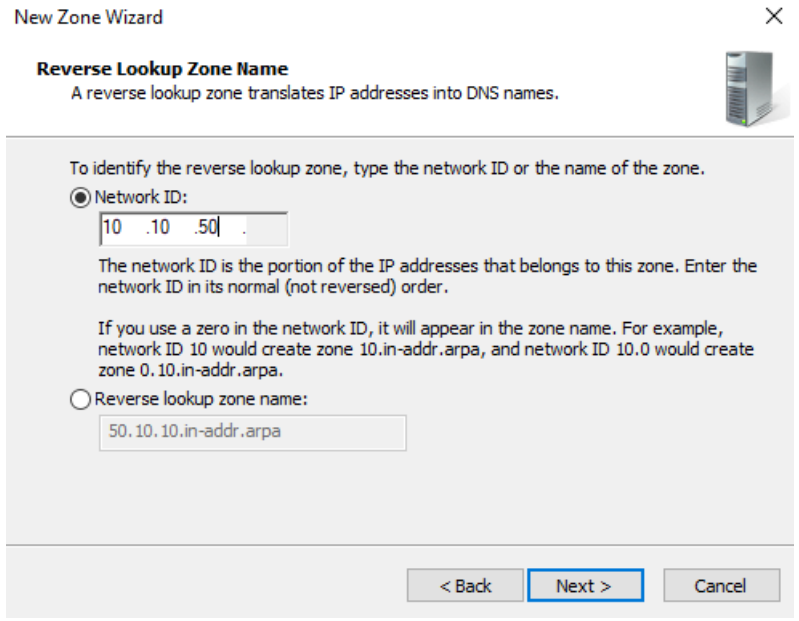
➢ Chọn vào Primary Zone:

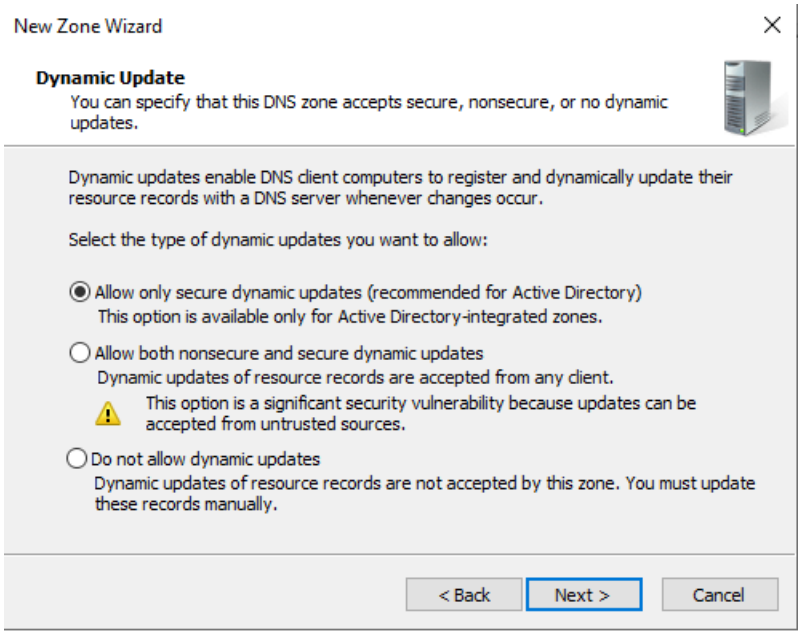


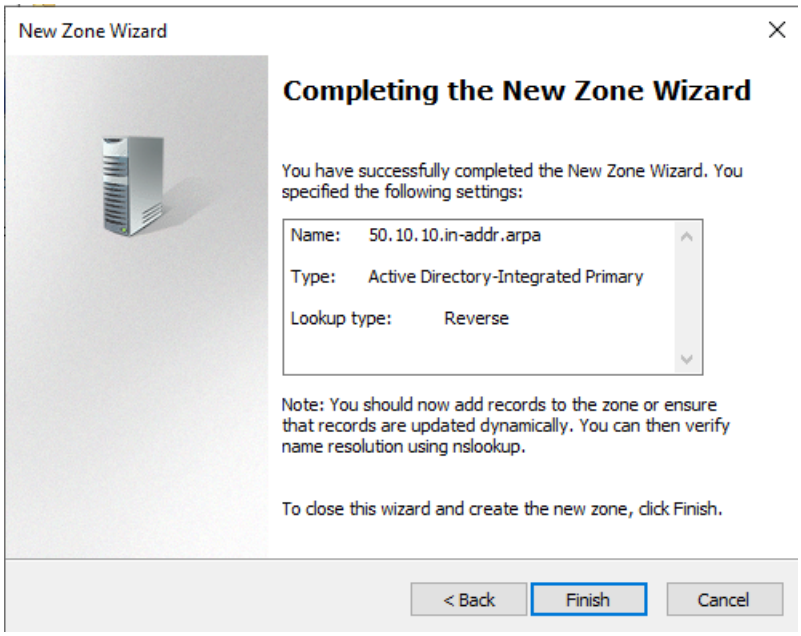
- Chọn IPv4:



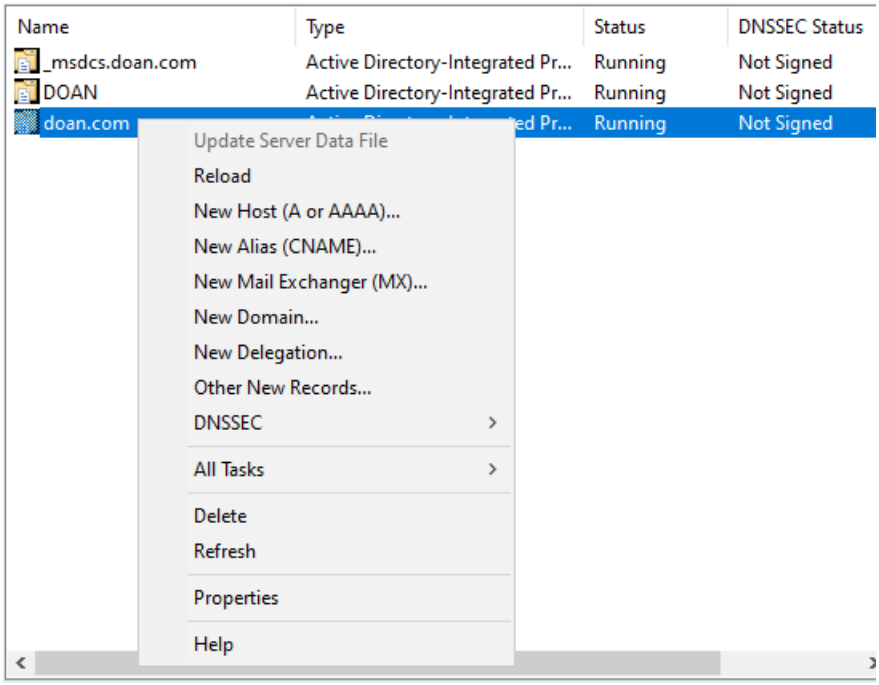
- Tới đây ta chọn vùng Network ID là 10.10.50.xxx, chọn vào Allow only…, chọn vào finish và kết thúc quá trình phân giải ngược tên miền


New Zone Wizard
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.
To identify the reverse lookup zone, type the network ID or the name of the zone.
Network ID:
10 .10 .50 .
The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.
If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.
Reverse lookup zone name:
50.10.10.in-addr.arpa
< Back
Next >
Cancel

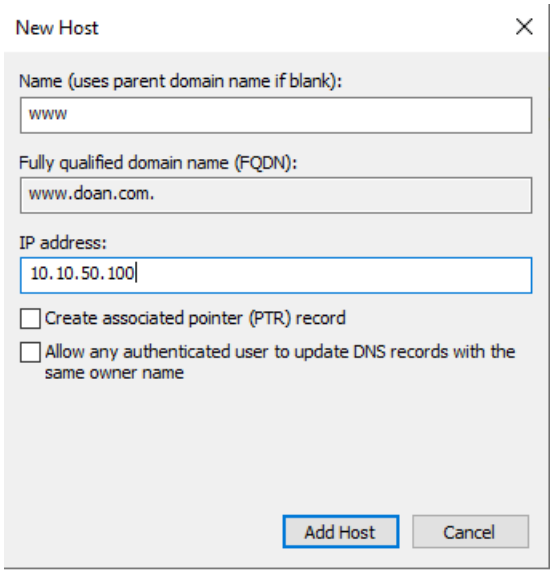

New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel



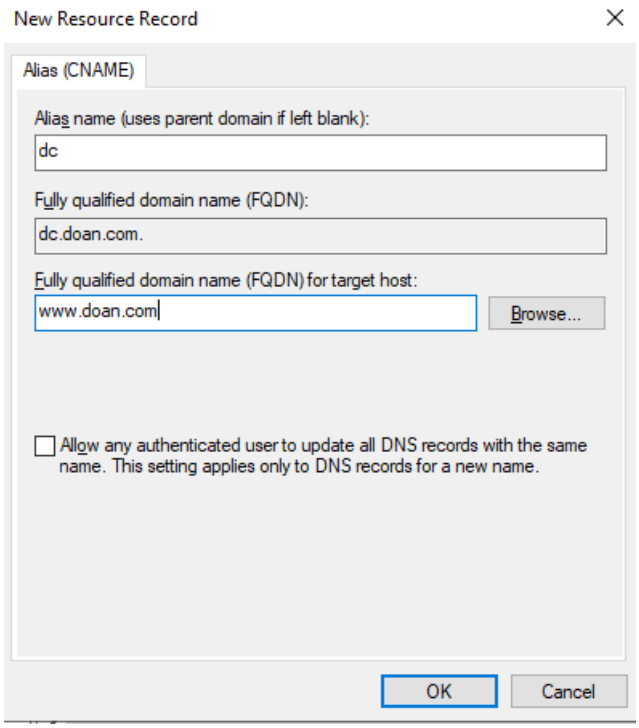
- Tạo new host bằng cách: ở mục Forward Lookup Zones nhấp chuột phải vào DNS doan.com → New Host



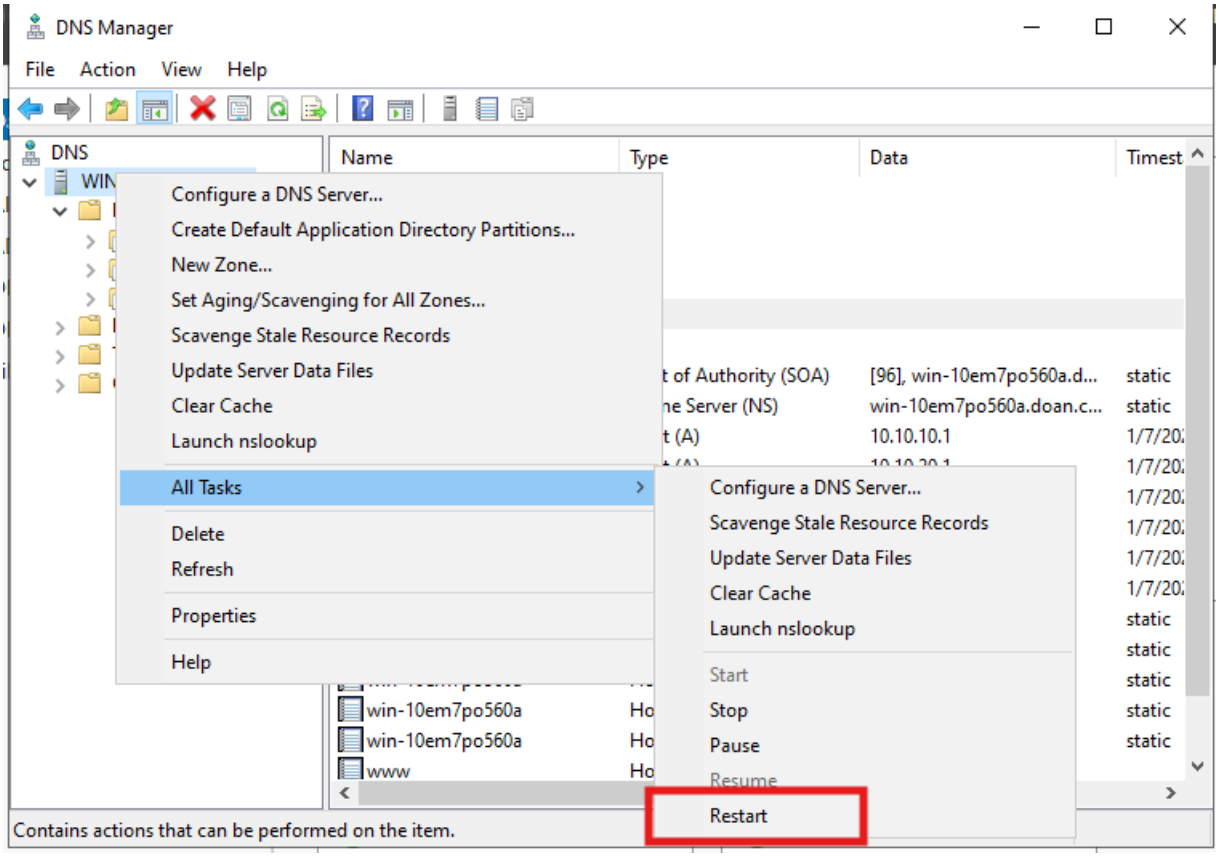
- Tạo New Host:



- Tạo Alias Host bằng cách: ở mục Forward Lookup Zones nhấp chuột phải vào DNS doan.com → Alias Host
- Tạo Alias Host:

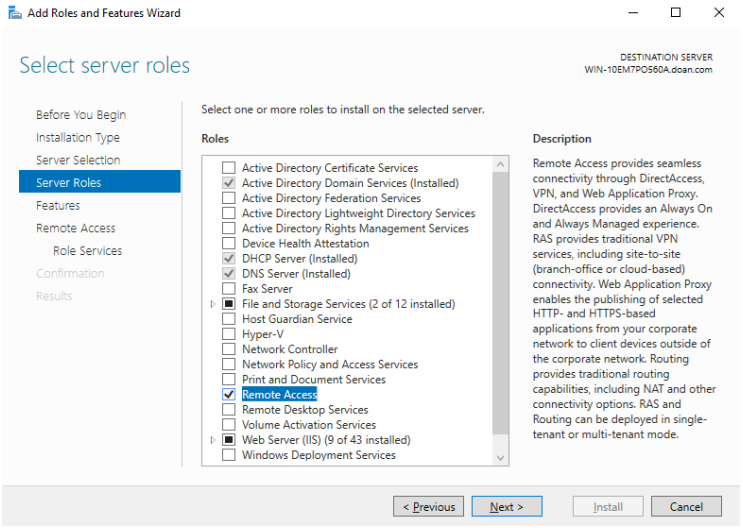


- Restart DNS:

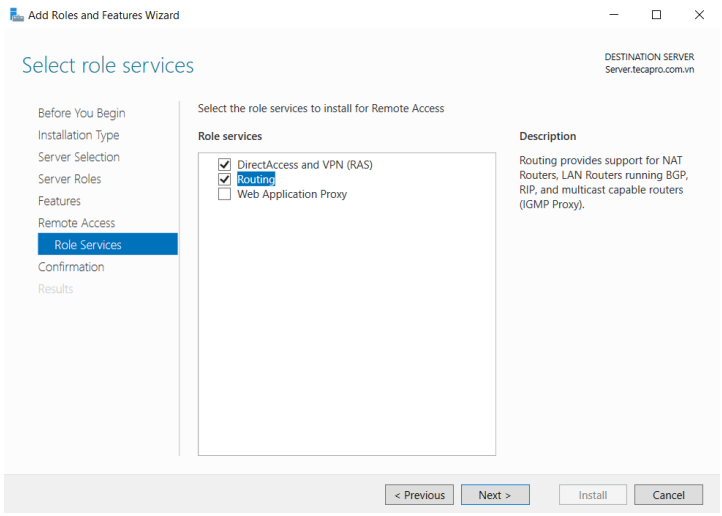

DNS Manager
File Action View Help
DNS
Name
Type
Data
Timest
Configure a DNS Server...
Create Default Application Directory Partitions...
New Zone...
Set Aging/Scavenging for All Zones...
Scavenge Stale Resource Records
Update Server Data Files
Clear Cache
Launch nslookup
All Tasks
Delete
Refresh
Properties
Help
Configure a DNS Server...
Scavenge Stale Resource Records
Update Server Data Files
Clear Cache
Launch nslookup
Start
Stop
Pause
Resume
Restart
win-10em7po560a
win-10em7po560a
www
Contains actions that can be performed on the item.

12. Cấu hình NAT

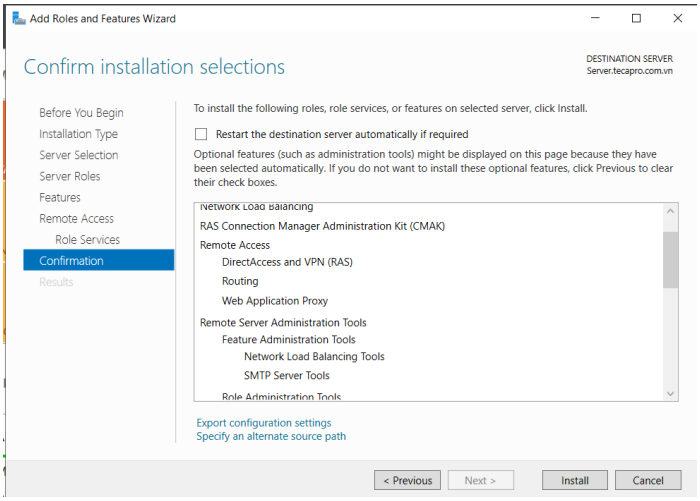
❖ Để cấu hình NAT, đầu tiên ta phải cài đặt Remote Access trong Server Manager



❖ Chọn vào Routing

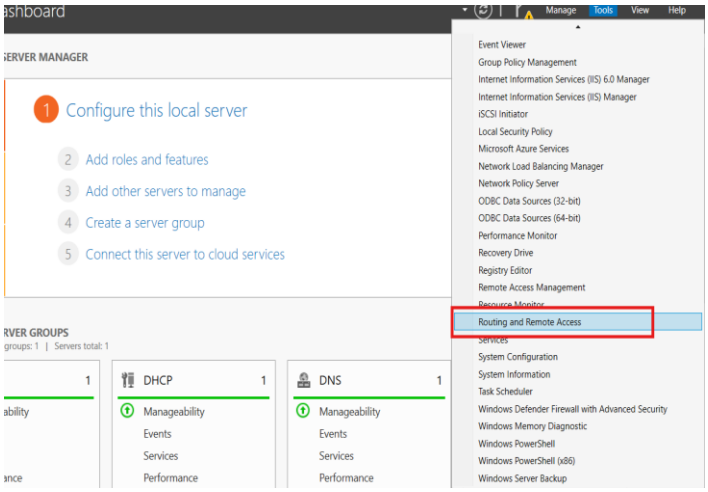


❖ Chọn Install để cài đặt

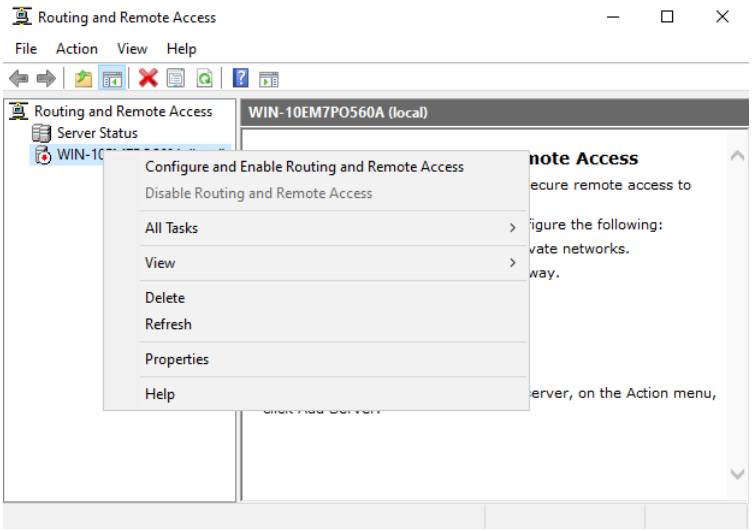


Hình 45: Cài đặt Routing

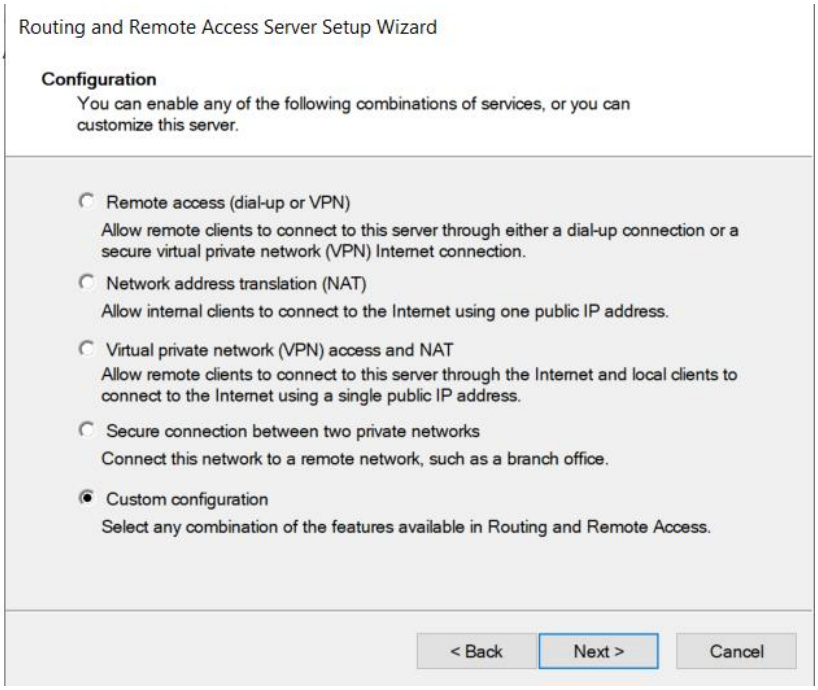
❖ Sau khi cài đặt xong, ta vào Tools → chọn Routing and Remote Access



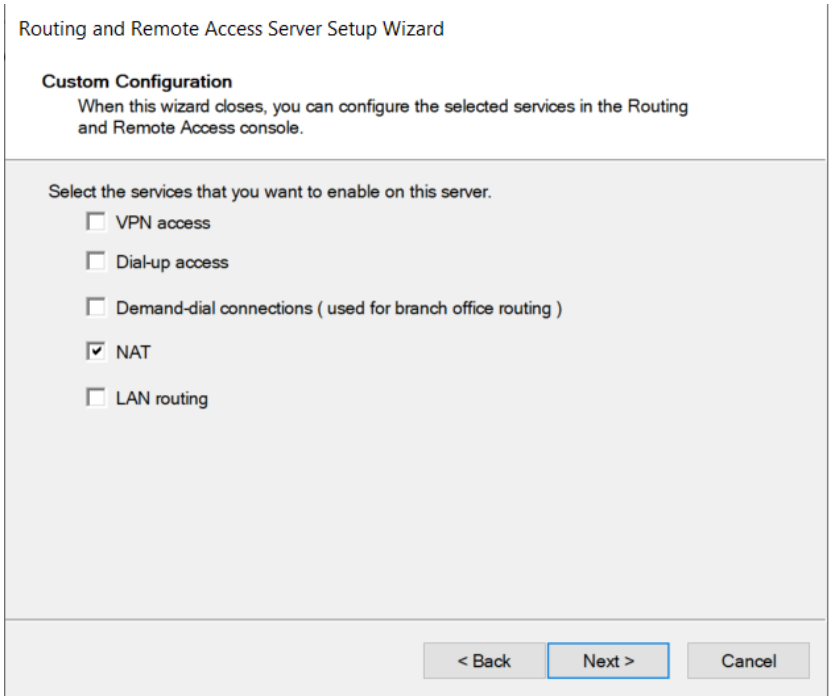
❖ Chuột phải vào server local → chọn Configure and Enable Routing and Remote Access



❖ Chọn Custom Configuration

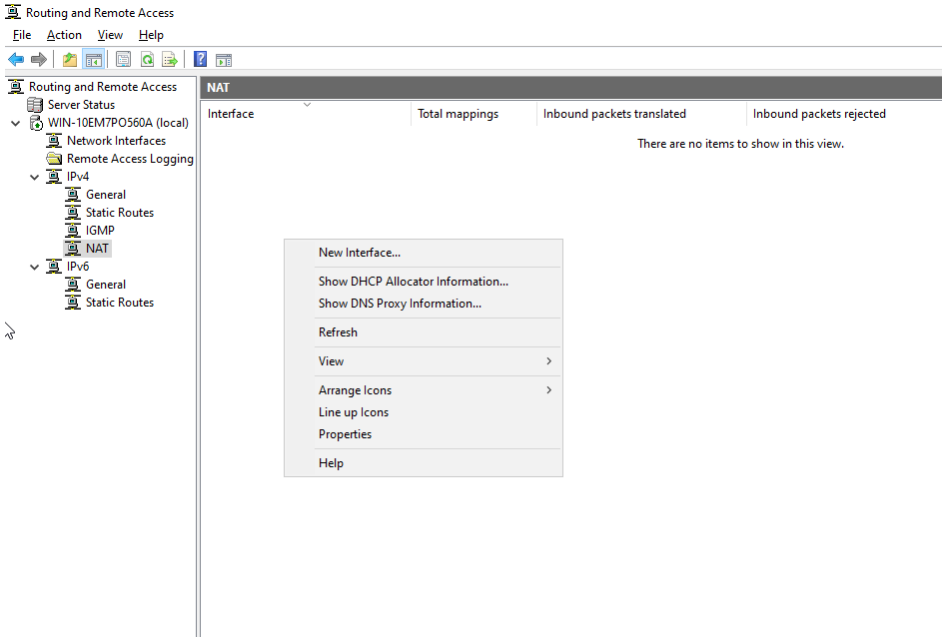


❖ Sau đó chọn NAT để hoàn thành thiết lập

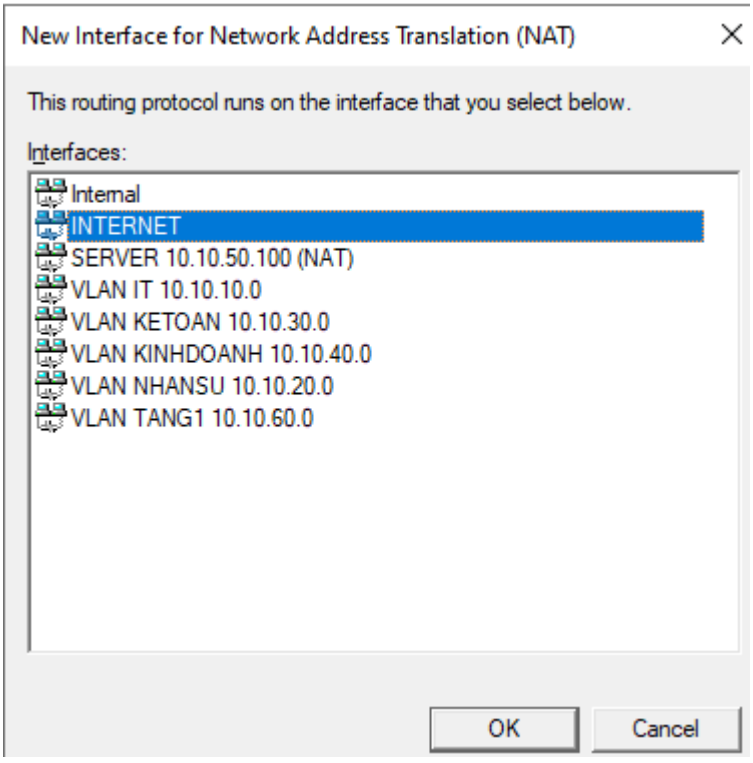


Hình 46: Thiết lập cơ chế NAT

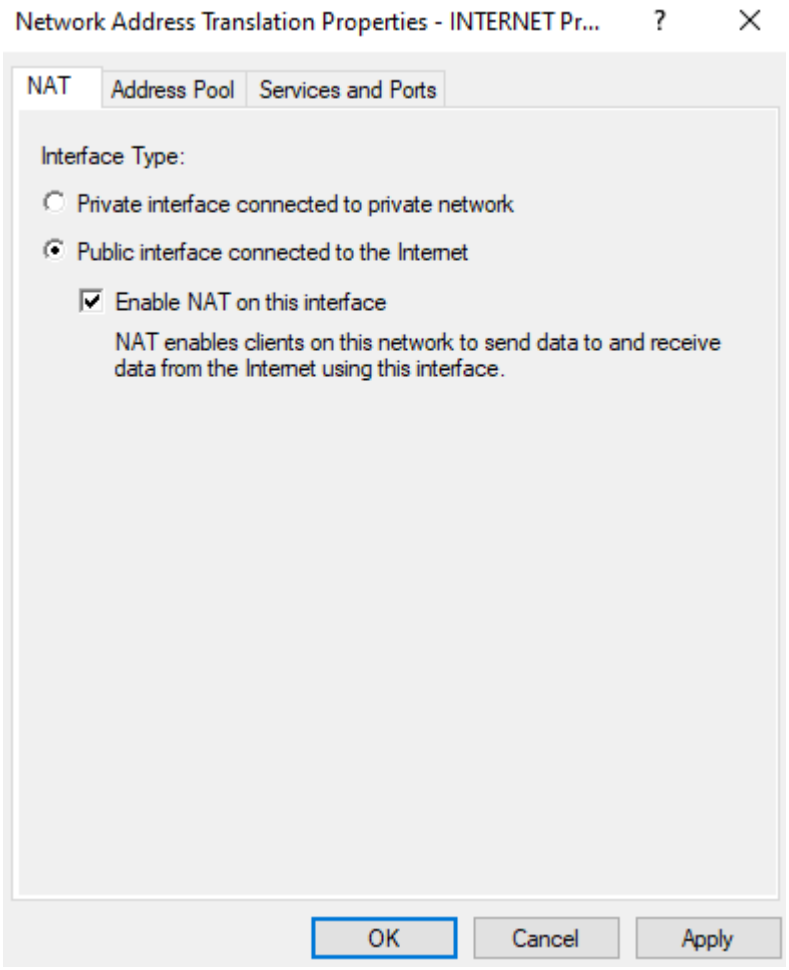
❖ Ở mục IPv4, ta chọn NAT, click chuột phải vào bảng trắng và chọn New Interface



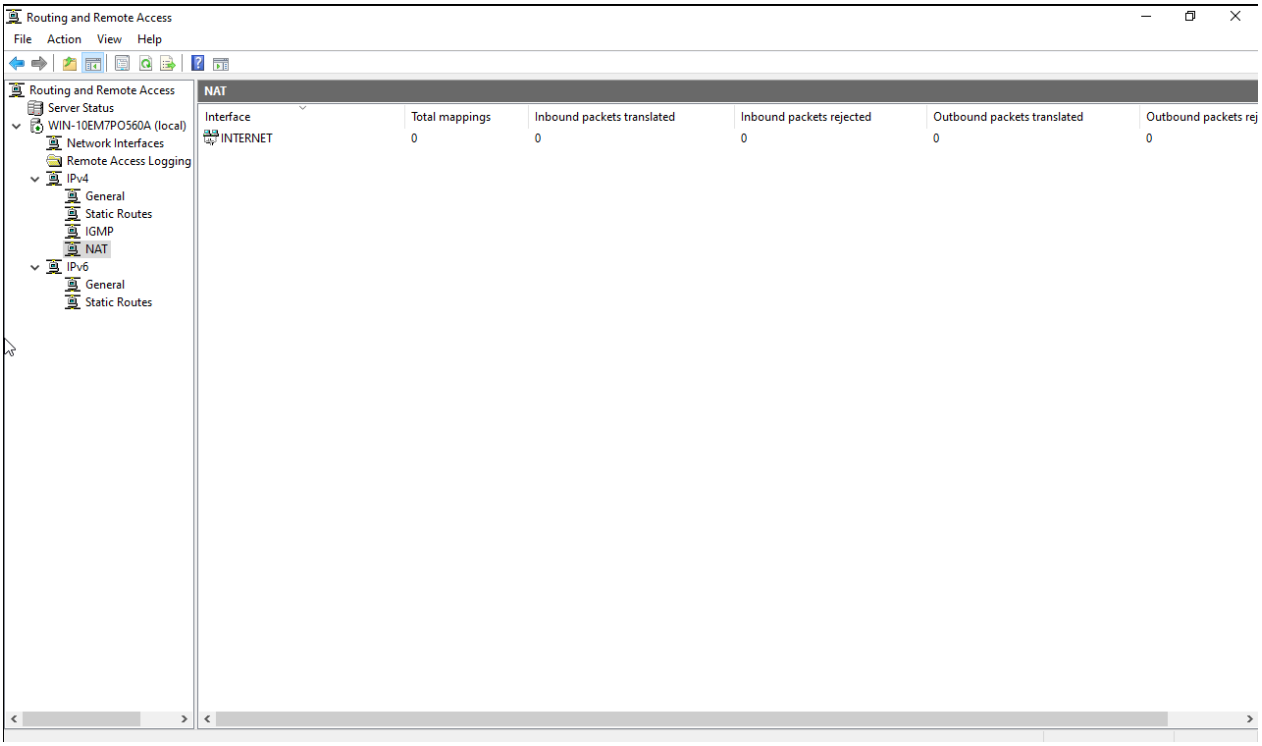
❖ Chọn card INTERNET



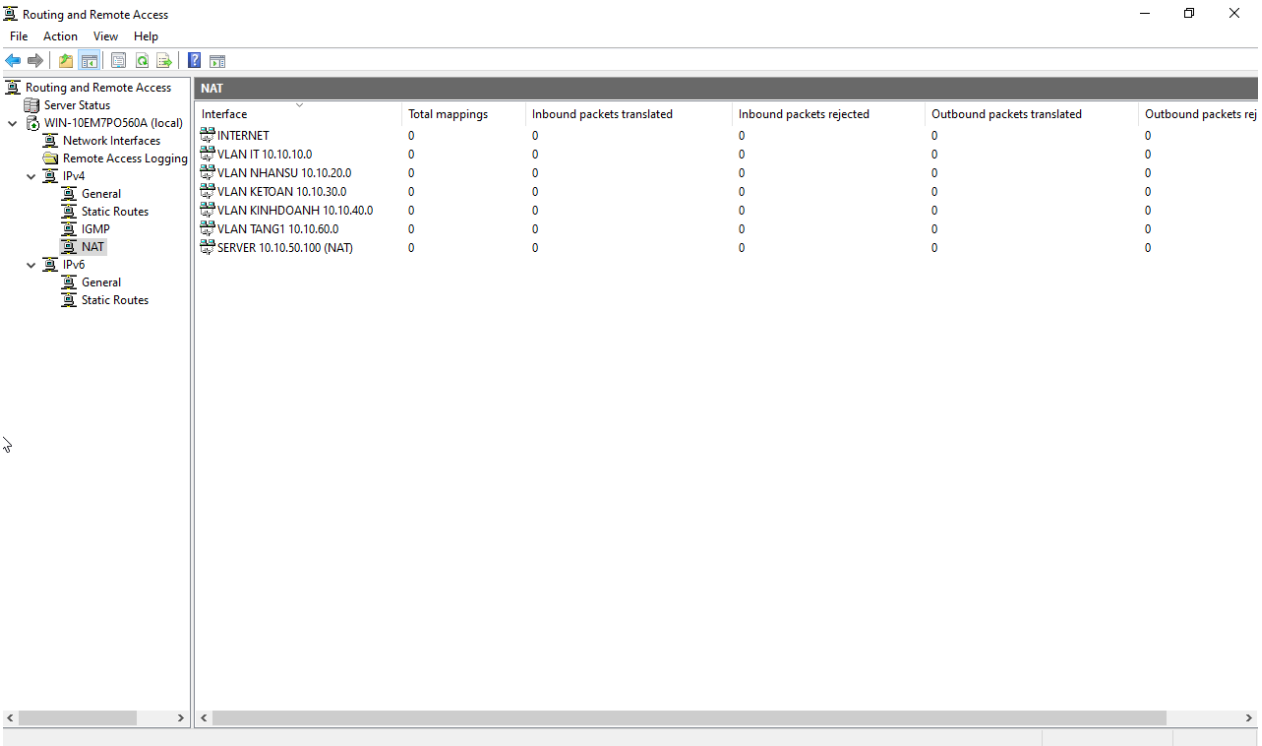
❖ Ở đây ta sẽ chọn vào Public interface và tích vào mục Enable NAT



❖ Nhấp vào OK, ta được:

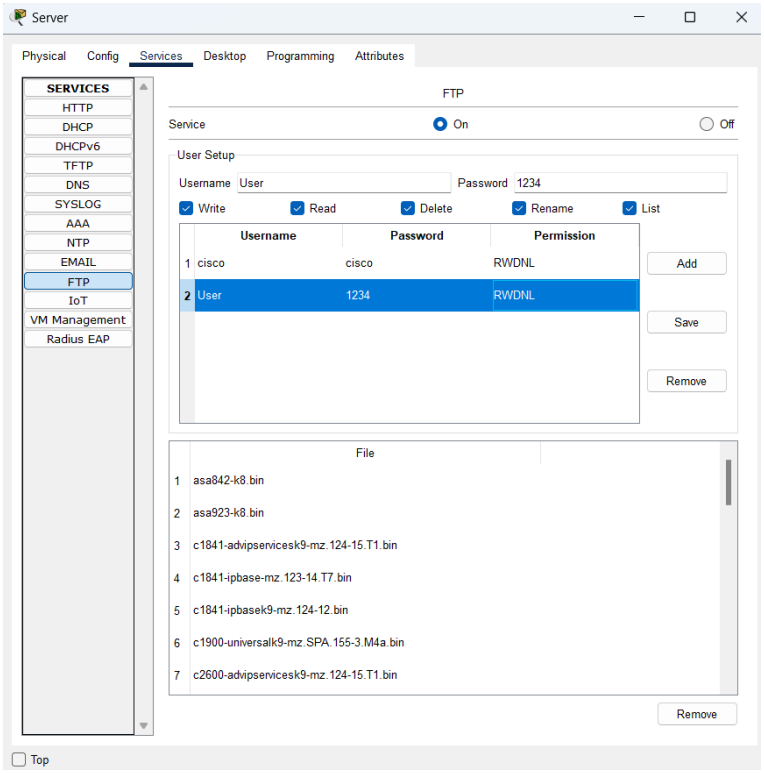


❖ Tương tự với các card mạng khác, nhưng đối với các card mạng nội bộ ta chọn vào Private interface



13. Cấu hình dịch vụ FTP

❖ Vào Server → vào tab Services → vào FTP để bật ON, tạo Username: user, password: 1234, cấp tất cả quyền



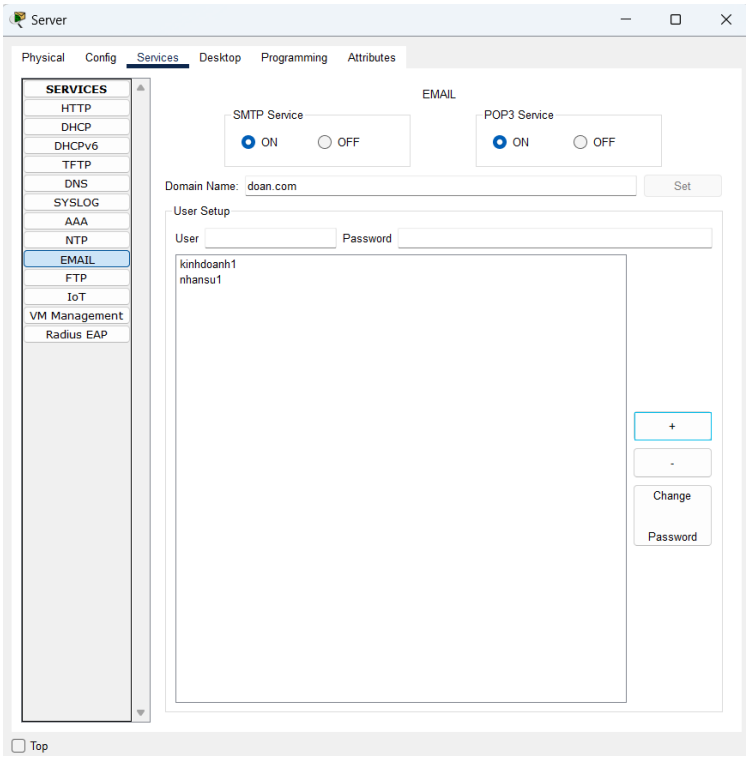
Hình 47: Cấu hình dịch vụ FTP

14. Cấu hình dịch vụ Mail Server

❖ Vào Server → vào tab Services → vào EMAIL để bật ON, tạo Domain name: doan.com -> Set

❖ Tạo 2 tài khoản:

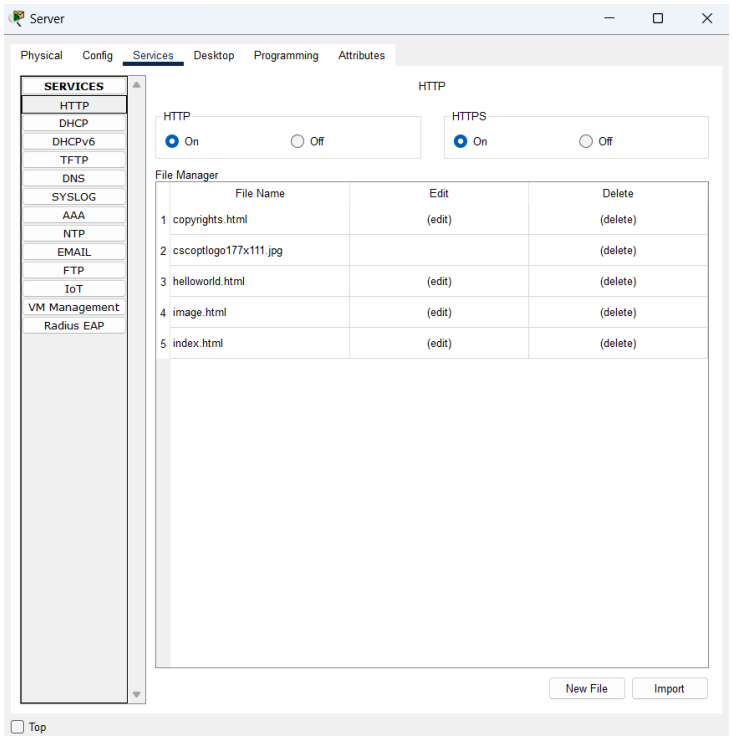
- ➢ kinhdoanh1 – password:1234
- ➢ ketoan1 - password:1234



Hình 48: Cấu hình dịch vụ Mail Server

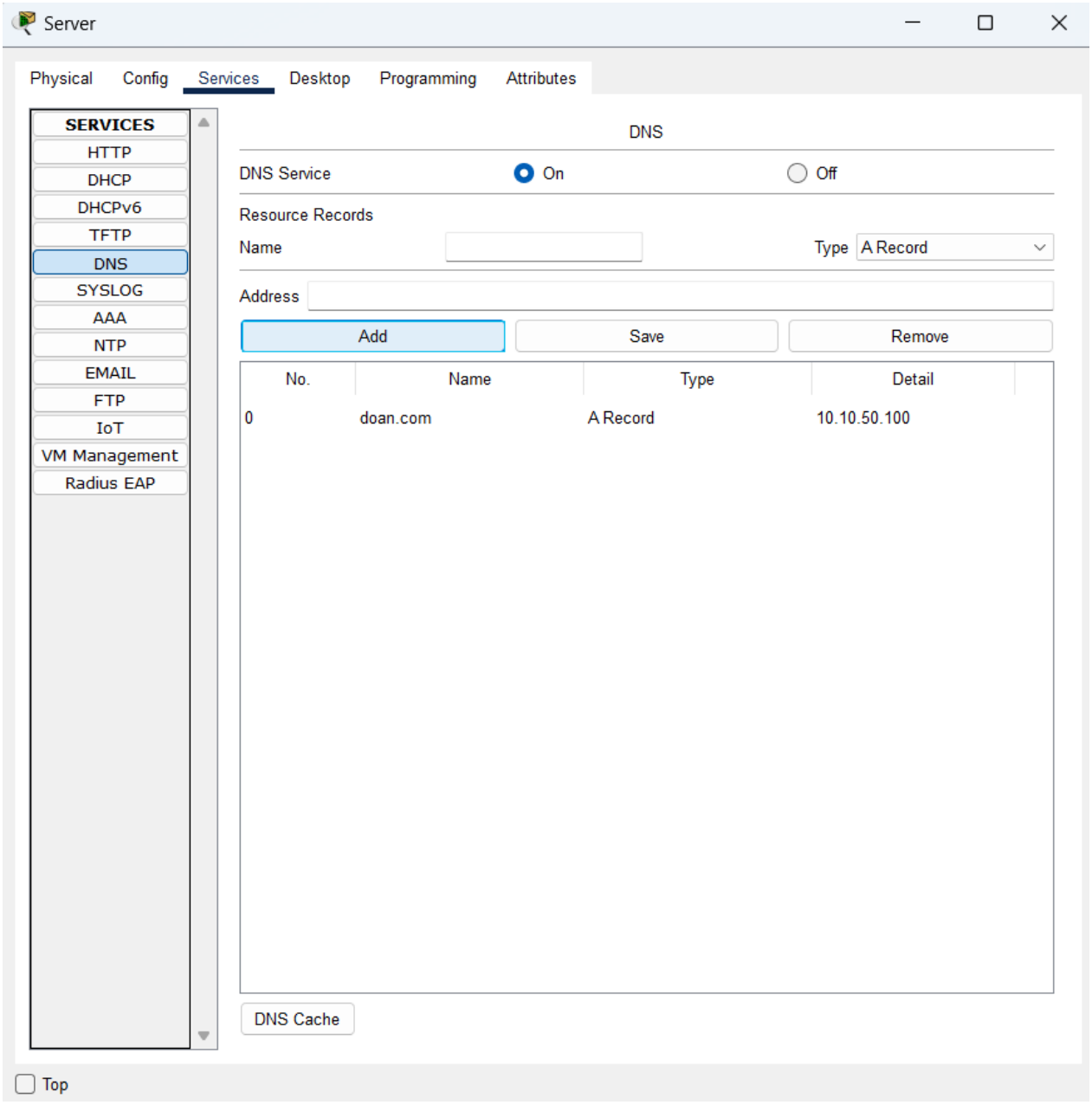
15. Cấu hình dịch vụ Web Server

❖ Vào Server → vào tab Services → vào HTTP để bật ON



Hình 49: Cấu hình dịch vụ Web Server

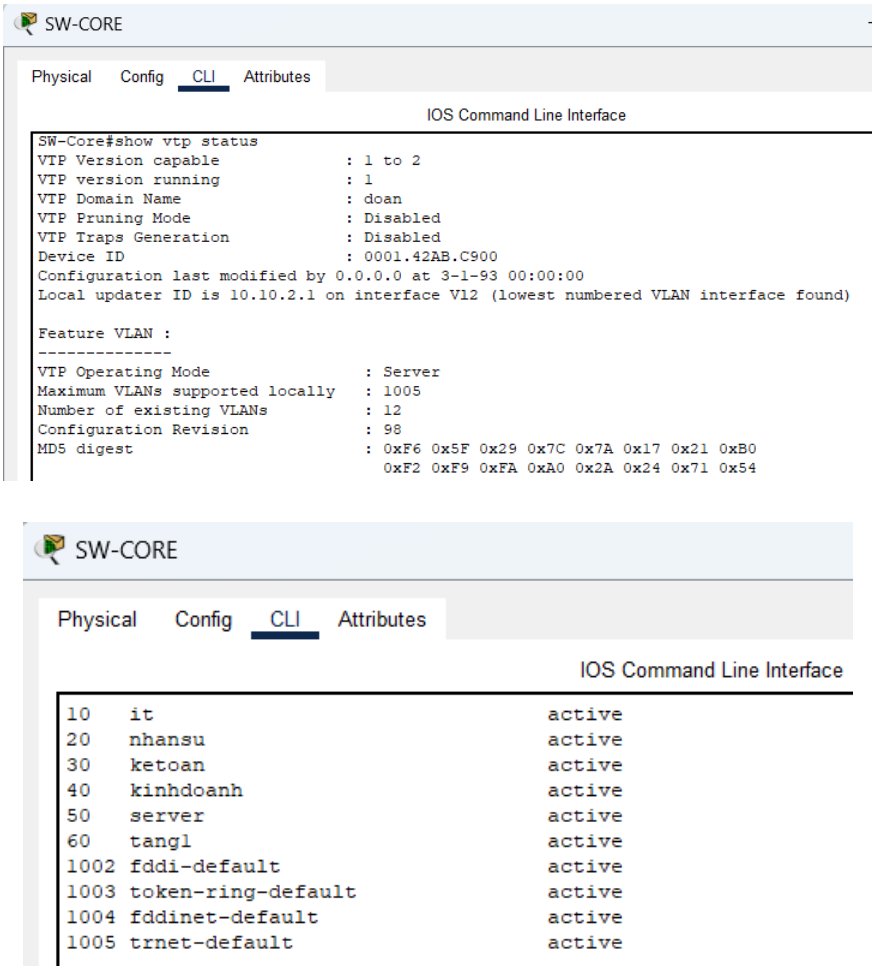
❖ Vào DNS tạo 1 record có tên là doan.com địa chỉ là của Server



II. Vận hành và kiểm thử

1. Kiểm thử VTP

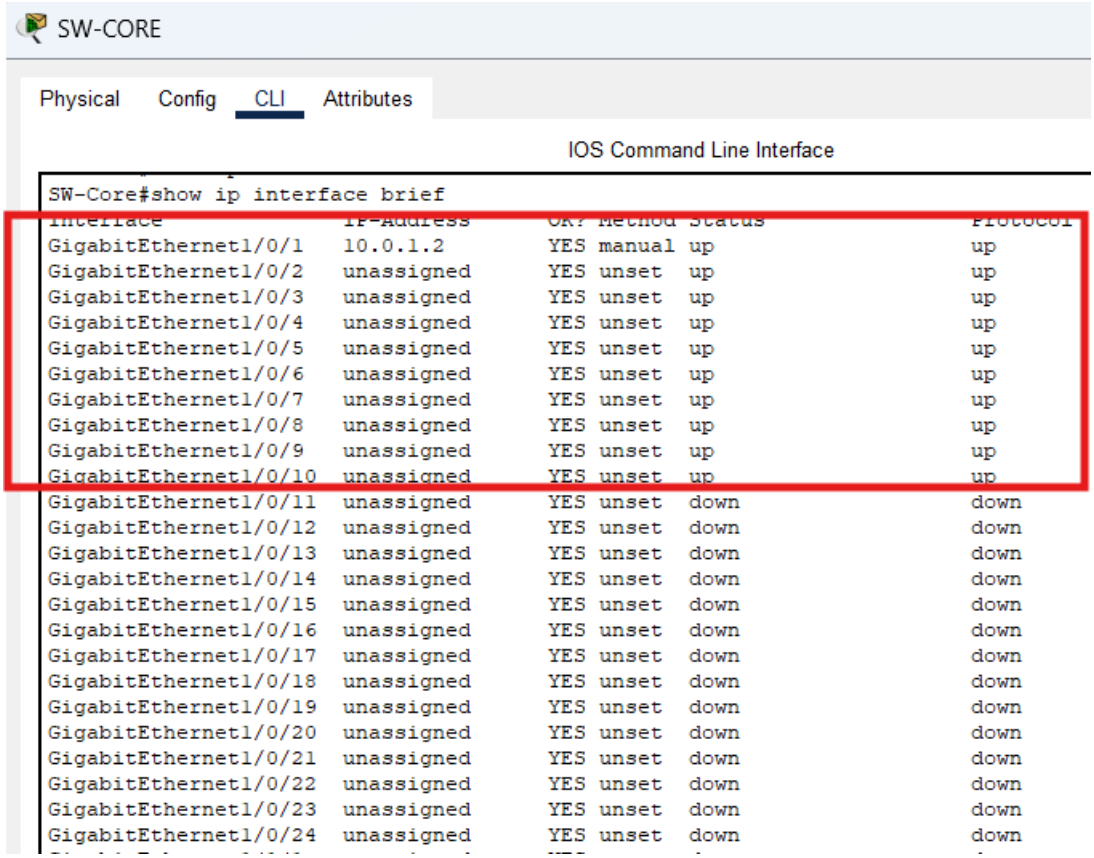
❖ Trên SW-Core-1, sau khi cấu hình xong ta kiểm tra bằng lệnh: “show vtp status” và “show VLAN” để kiểm tra, ta được các VLAN 10 đến 60, vtp ở chế độ Server:



Hình 50: Kiểm thử VTP

2. Kiểm thử Trucking

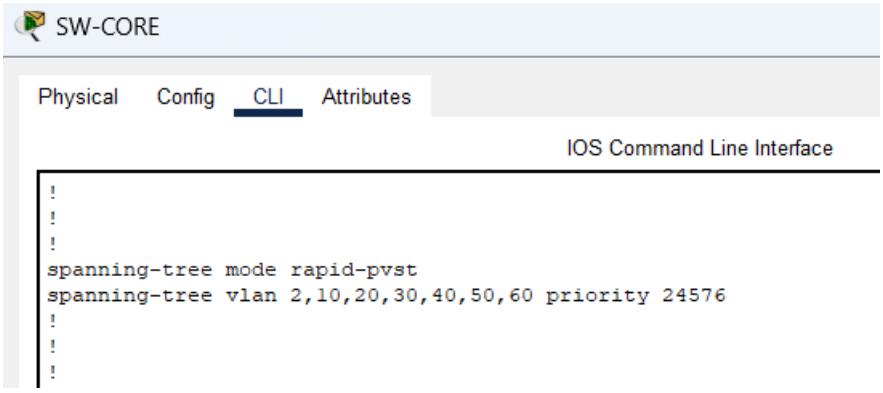
❖ Đầu tiên, ta sẽ kiểm tra trunking các port nối giữa switch core và switch access, ta kiểm tra bằng lệnh: “show ip interface brief” và “show run”, ta thấy các cổng nối giữa switch core và các switch access đã được up, đồng thời các cổng đã bật mode trunk.



Hình 51: Kiểm thử Trunking

3. Kiểm thử STP

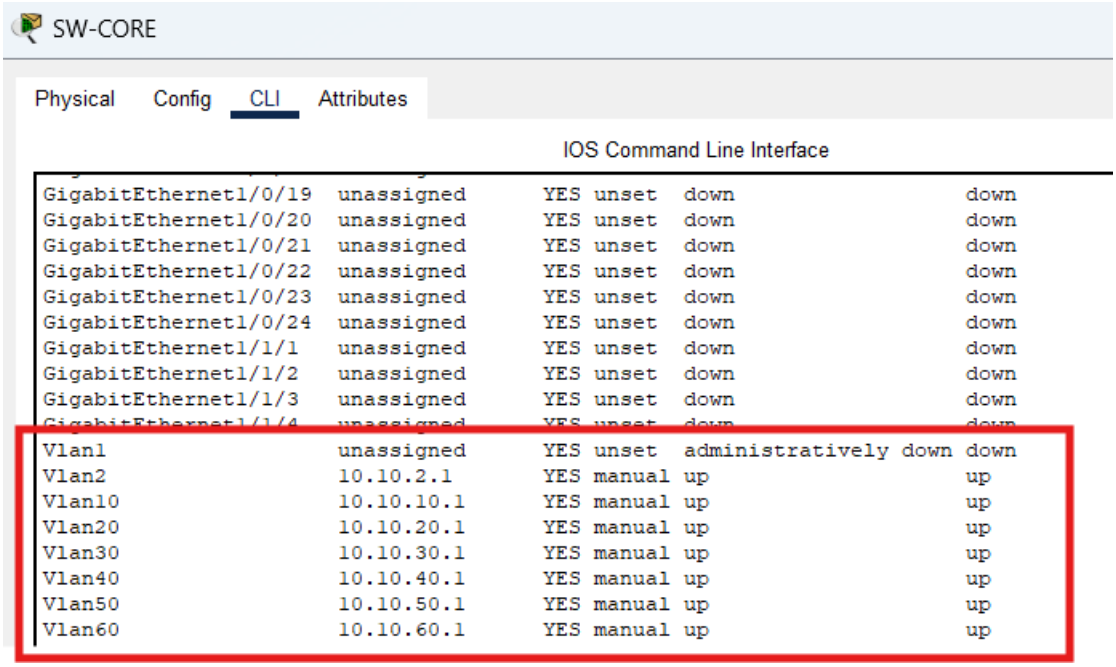
❖ Ta sử dụng lệnh: "show run" để kiểm tra trên SW-Core



Hình 52: Kiểm thử STP

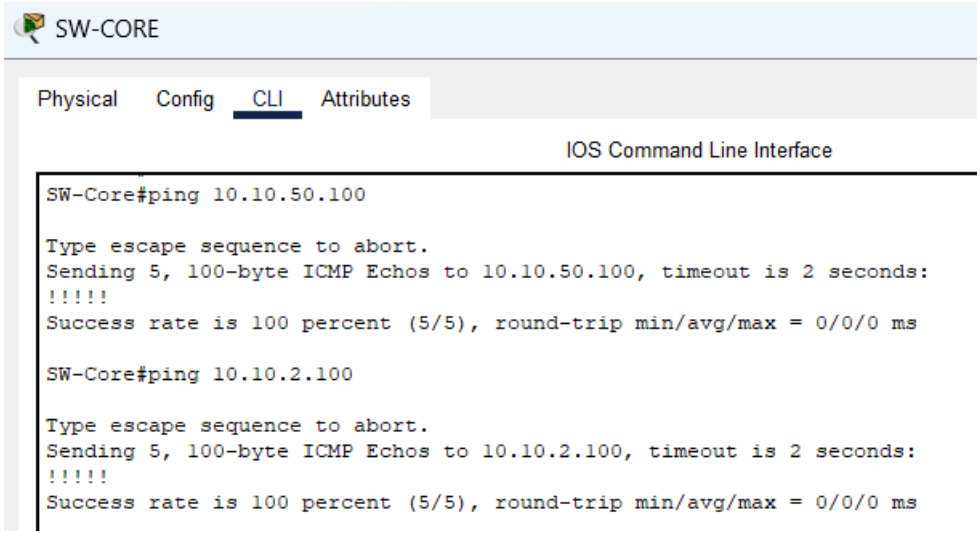
4. Kiểm thử cấp địa chỉ IP

❖ Sau khi cấu hình IP trên Switch Core, ta dùng lệnh "show ip interface brief" để kiểm tra và thấy các VLAN đã được cấp IP



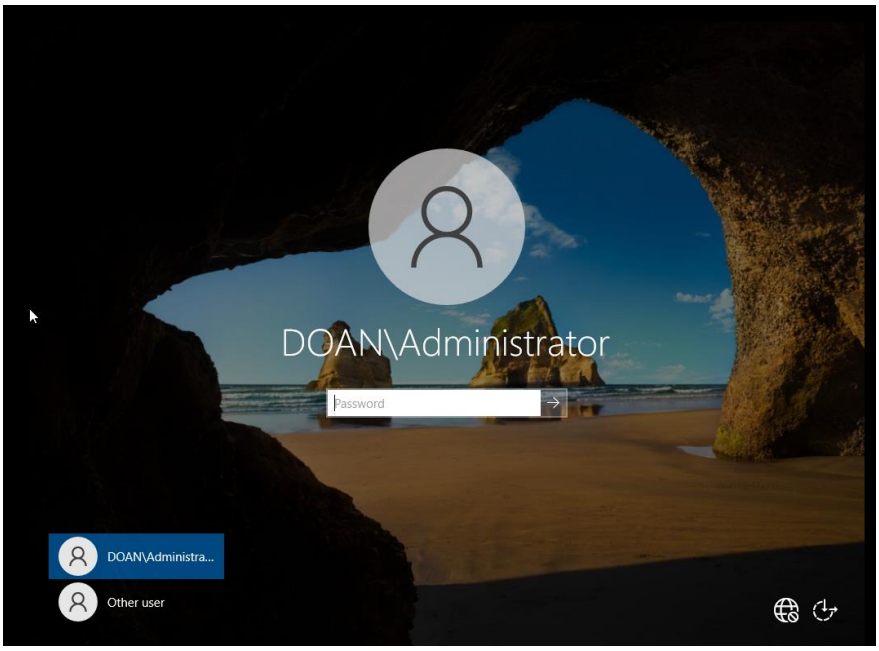
Hình 53: Kiểm thử địa chỉ IP

- Ta dùng Switch-Core và sử dụng lệnh: "ping 10.10.50.100" và "ping 10.10.2.100" để ping kiểm tra địa chỉ IP của Server và Wireless



5. Kiểm thử dịch vụ Domain Controller

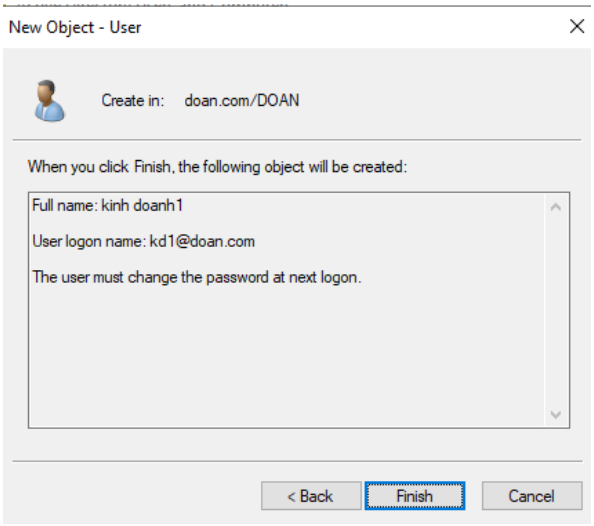
❖ Sau khi cài đặt xong, Server sẽ yêu cầu ta Restart máy, và đây là giao diện sau khi nâng cấp lên Domain Controller: Server sẽ lên quyền Administrator kèm theo tên domain



Hình 54: Kiểm thử Domain

6. Kiểm thử tạo User

❖ Sau khi tạo xong User:

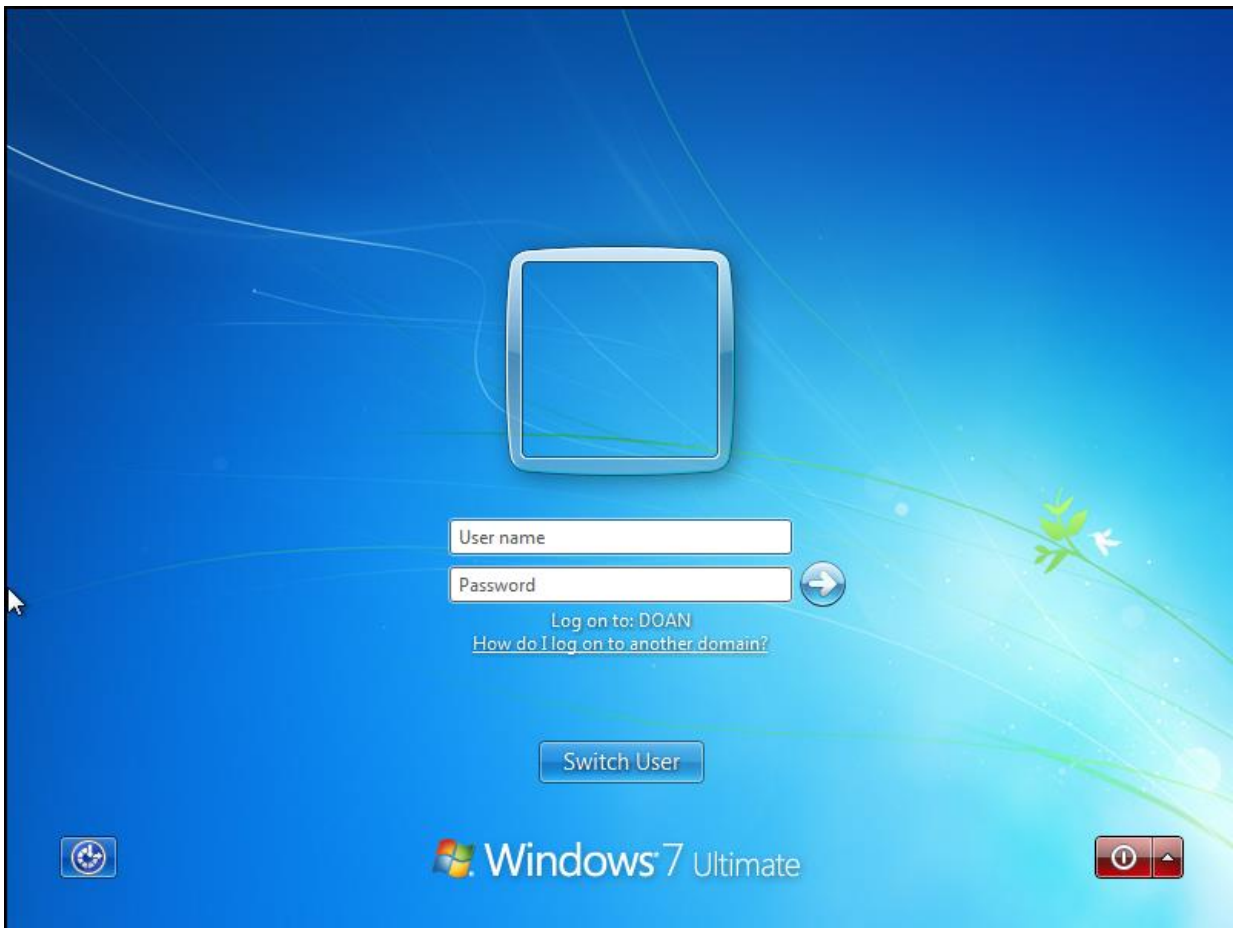


Name	Type	Description
IT	Security Group...	
ke toan 1	User	
ke toan 2	User	
KETOAN	Security Group...	
kinh doanh1	User	
KINHDOANH	Security Group...	
NHANSU	Security Group...	
TANG1	Security Group...	

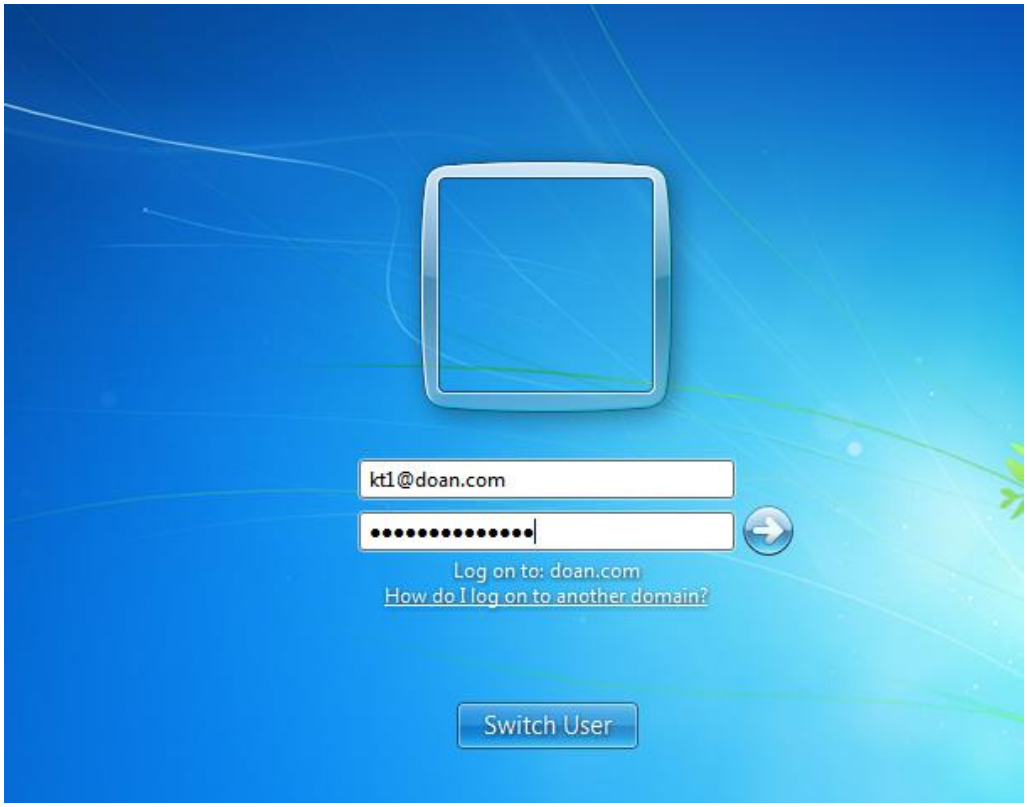
Hình 55: Kiểm thử việc tạo User

7. Kiểm thử Join Client vào Domain

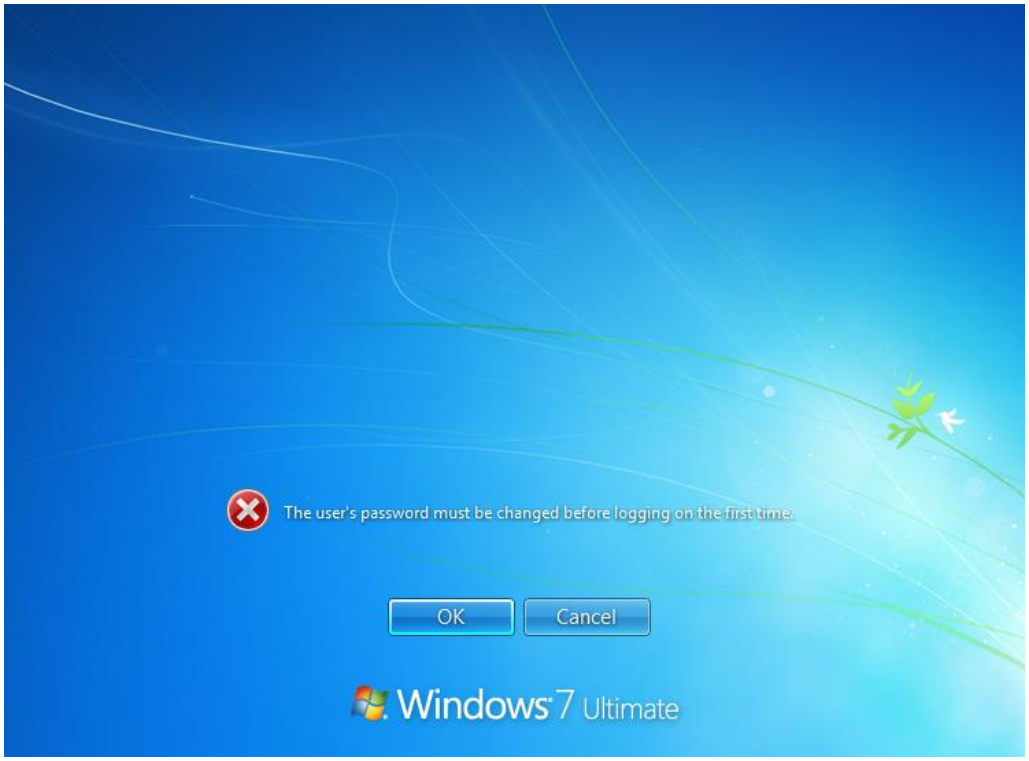
❖ Màn hình đăng nhập của client sau khi join vào domain



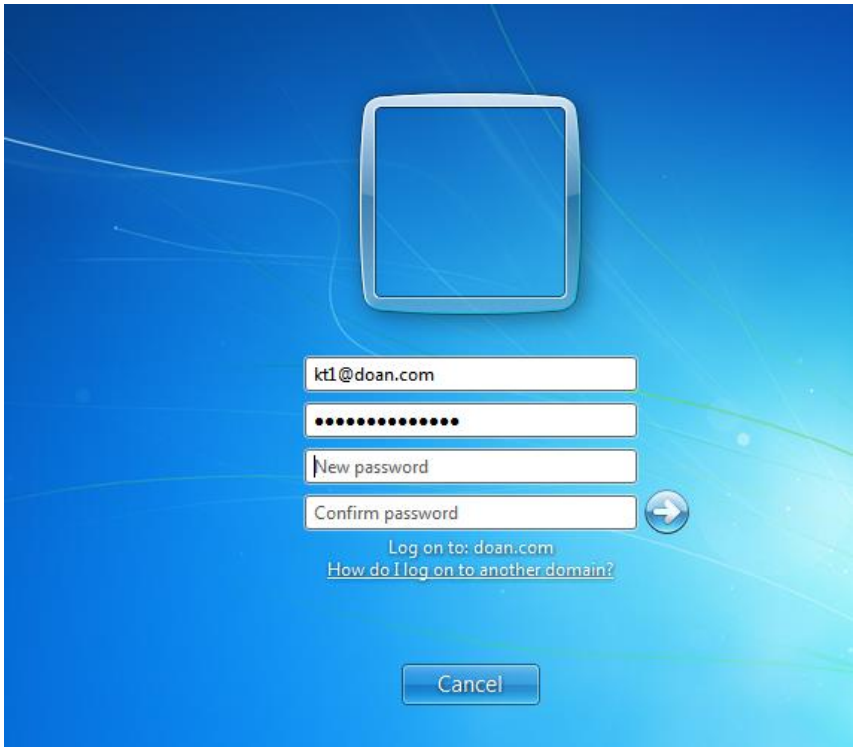
❖ Lúc này ta sẽ đăng nhập vào client bằng user đã được tạo trên server



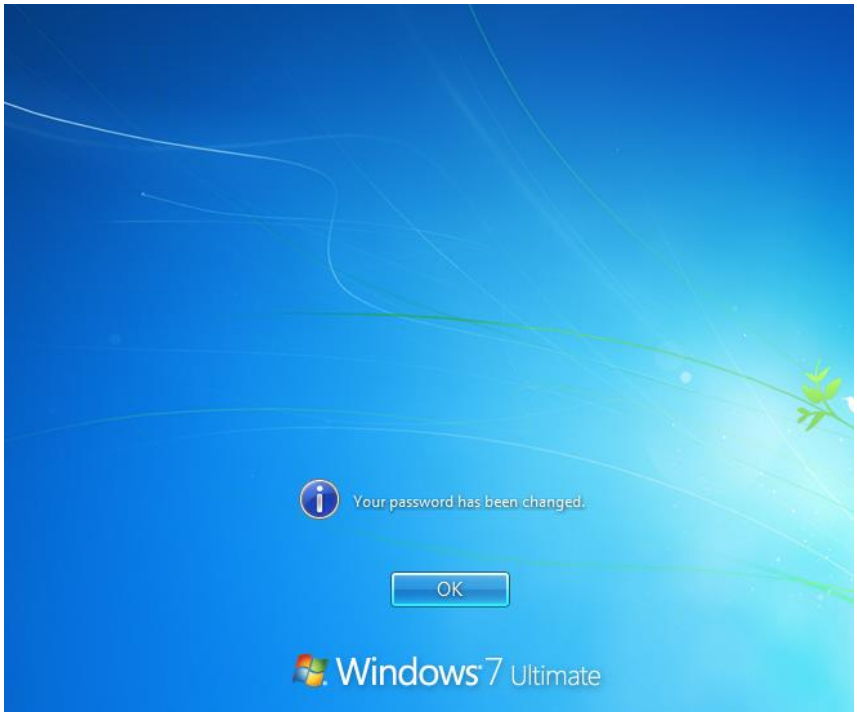
❖ Sau khi đăng nhập hệ thống sẽ yêu cầu đổi password



❖ Ta tạo password mới với đủ độ phức tạp



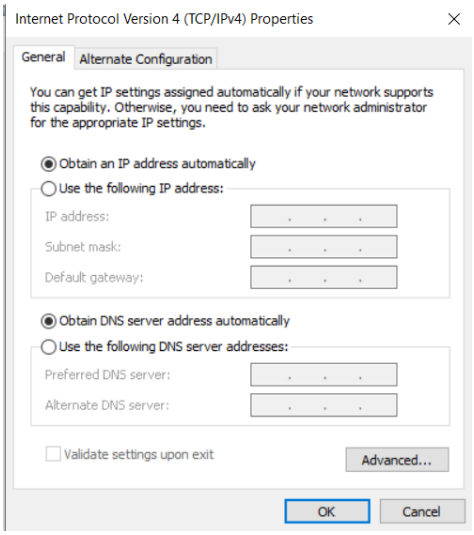
❖ Thay đổi password thành công



❖ Tương tự, ta cũng sẽ join domain cho các client khác và đăng nhập bằng nhập bằng các user đã tạo.

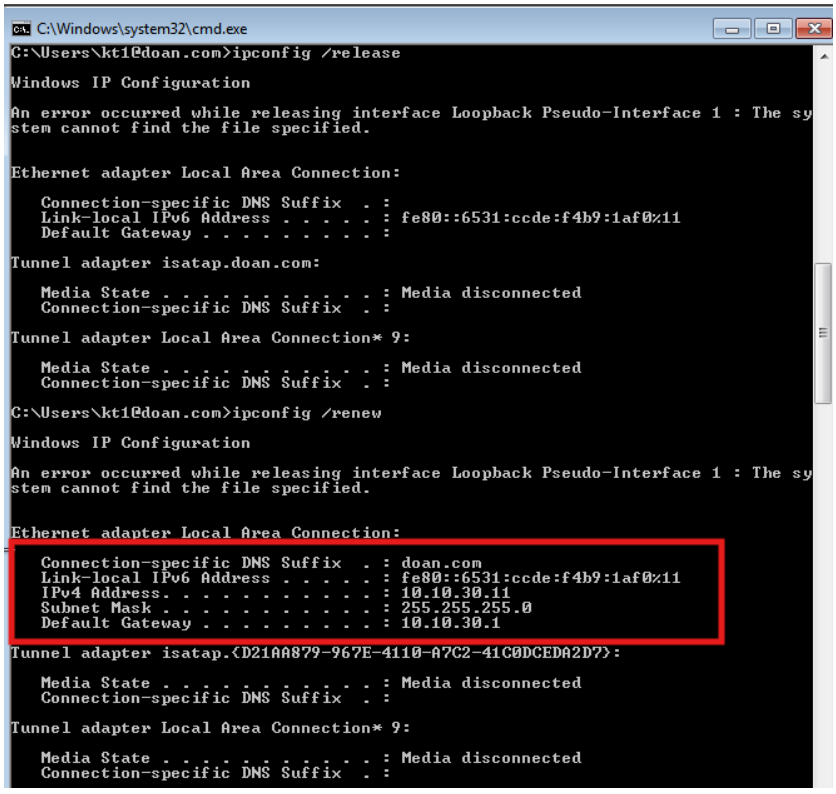
8. Kiểm thử DHCP

❖ Sau khi cấu hình xong, ta qua các client mỗi phòng để cấp IP cho các máy. Đầu tiên, chuyển về dạng cấp IP động



❖ Vào Command Prompt, sử dụng lệnh ipconfig /release, và ipconfig /renew để reset và xin cấp IP

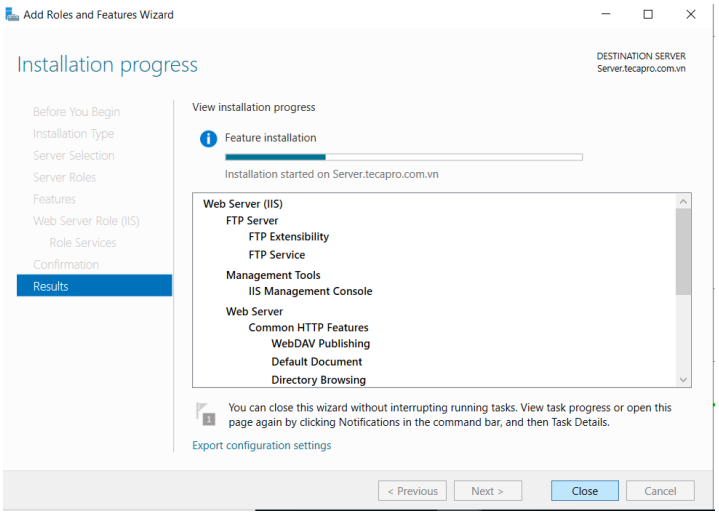
➢ Phòng Kế Toán: đã được cấp IP 10.10.30.11 thành công



Hình 56: Kiểm thử DHCP trên máy Client

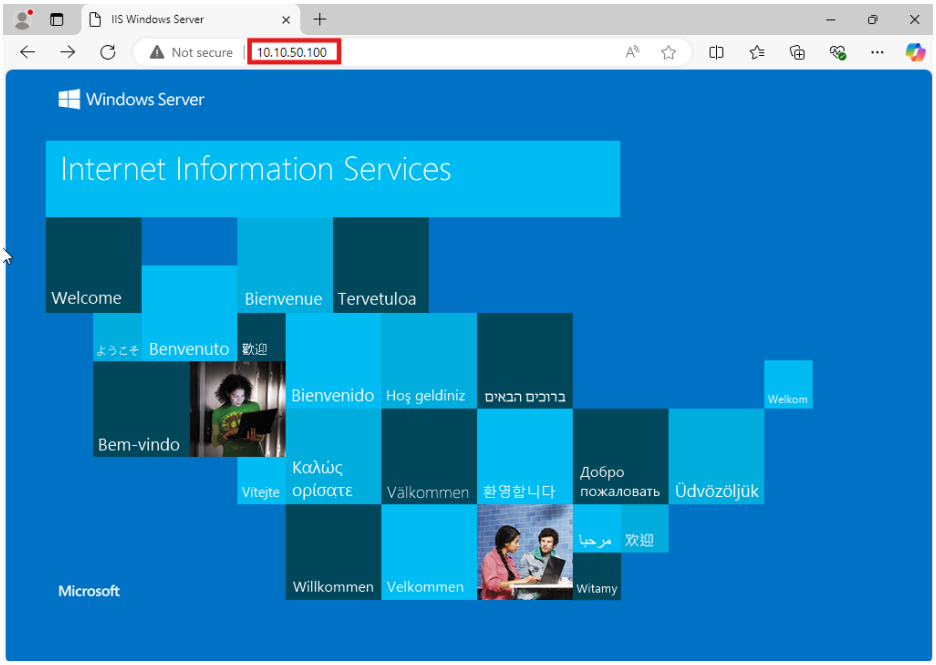
9. Kiểm thử DNS Server

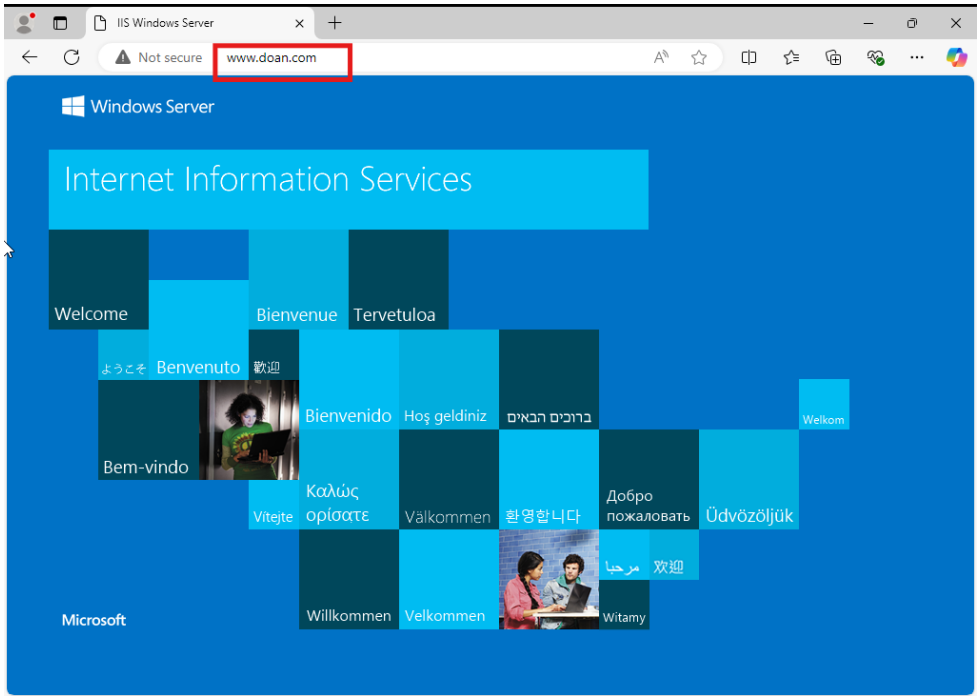
❖ Cài Web Server (IIS) để test dịch vụ



Hình 57: Cài đặt Web Server

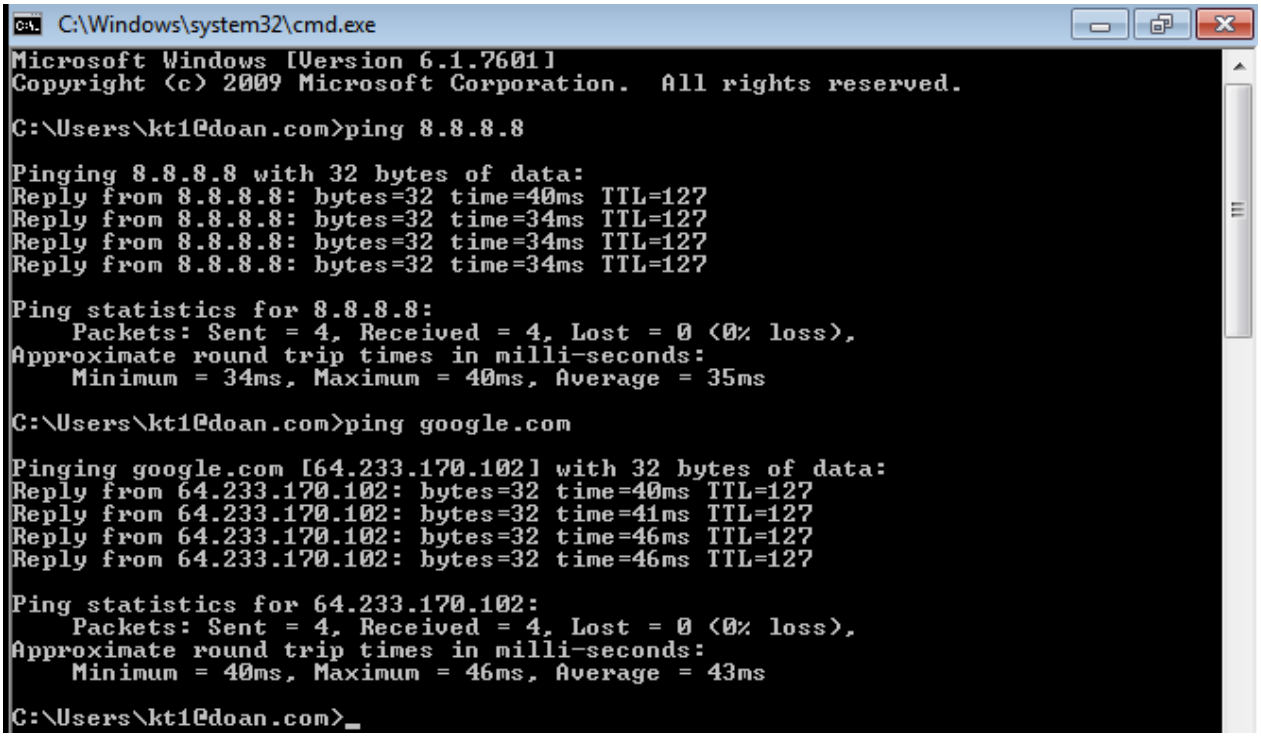
❖ Trên Server ta truy cập vào 10.10.40.100 và www.doan.com





10. Kiểm thử cấu hình NAT

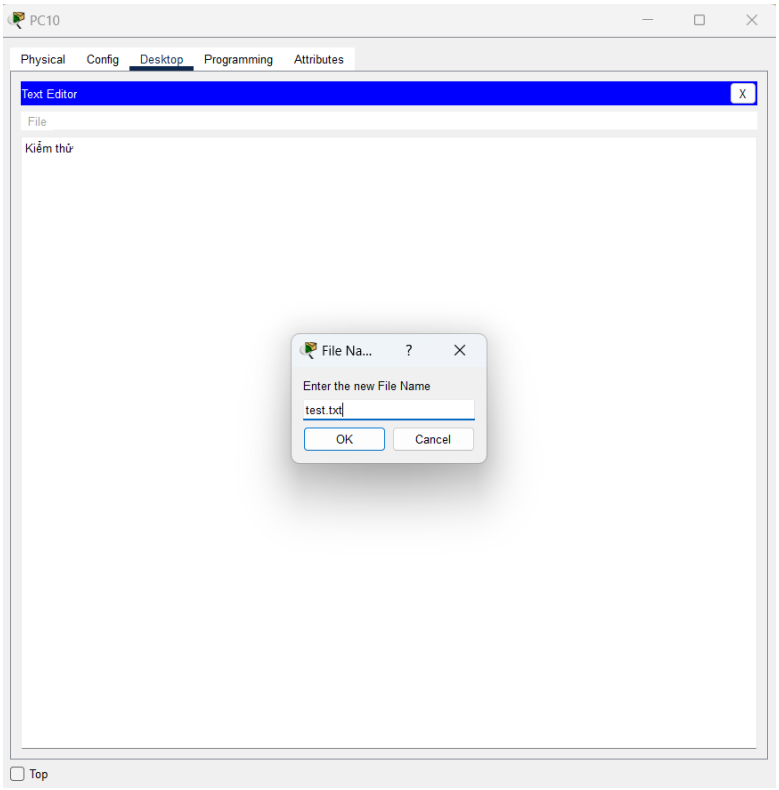
❖ Sau khi cấu hình xong, ta chuyển qua các máy client để ping kiểm tra thử, sử dụng lệnh: "ping 8.8.8.8", và "ping google.com"



Hình 58: Kiểm thử cấu hình NAT

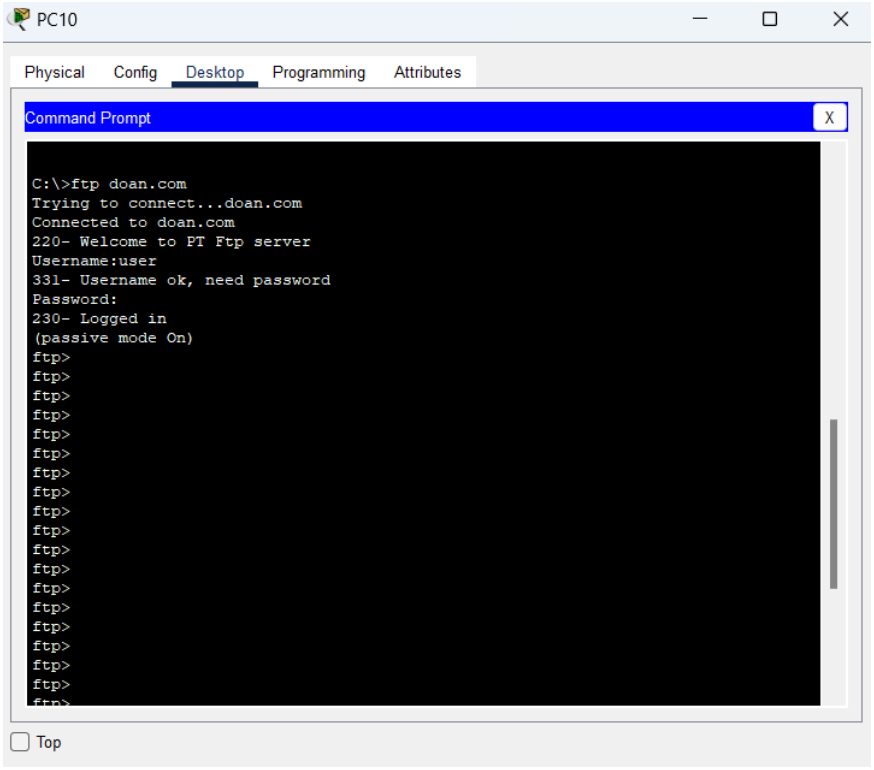
11. Kiểm thử dịch vụ FTP

❖ Qua máy client ta vào mục Text Editor để tạo 1 file và lưu lại

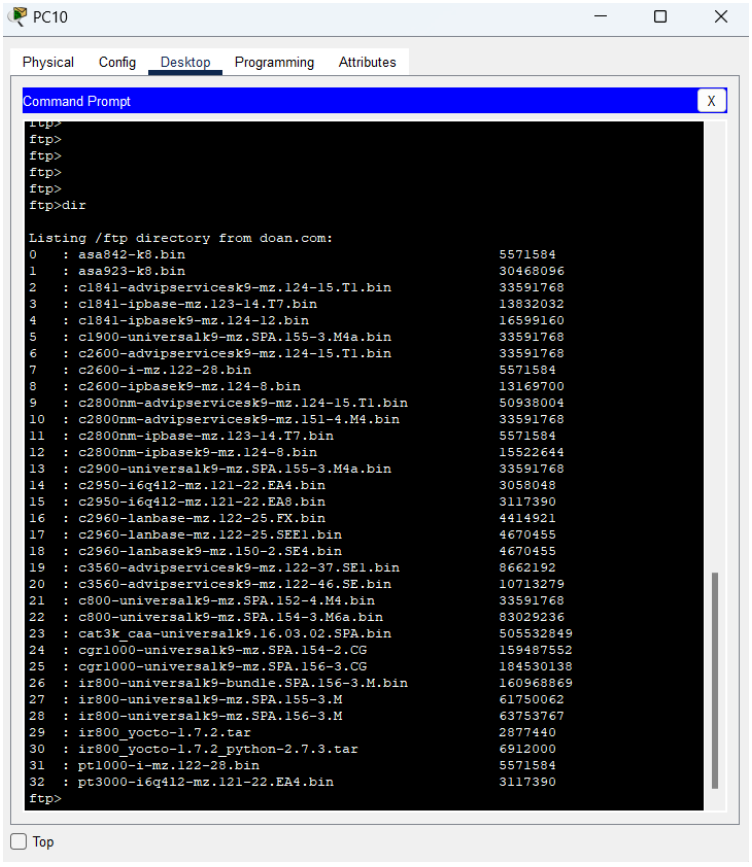


Hình 59: Kiểm thử dịch vụ FTP

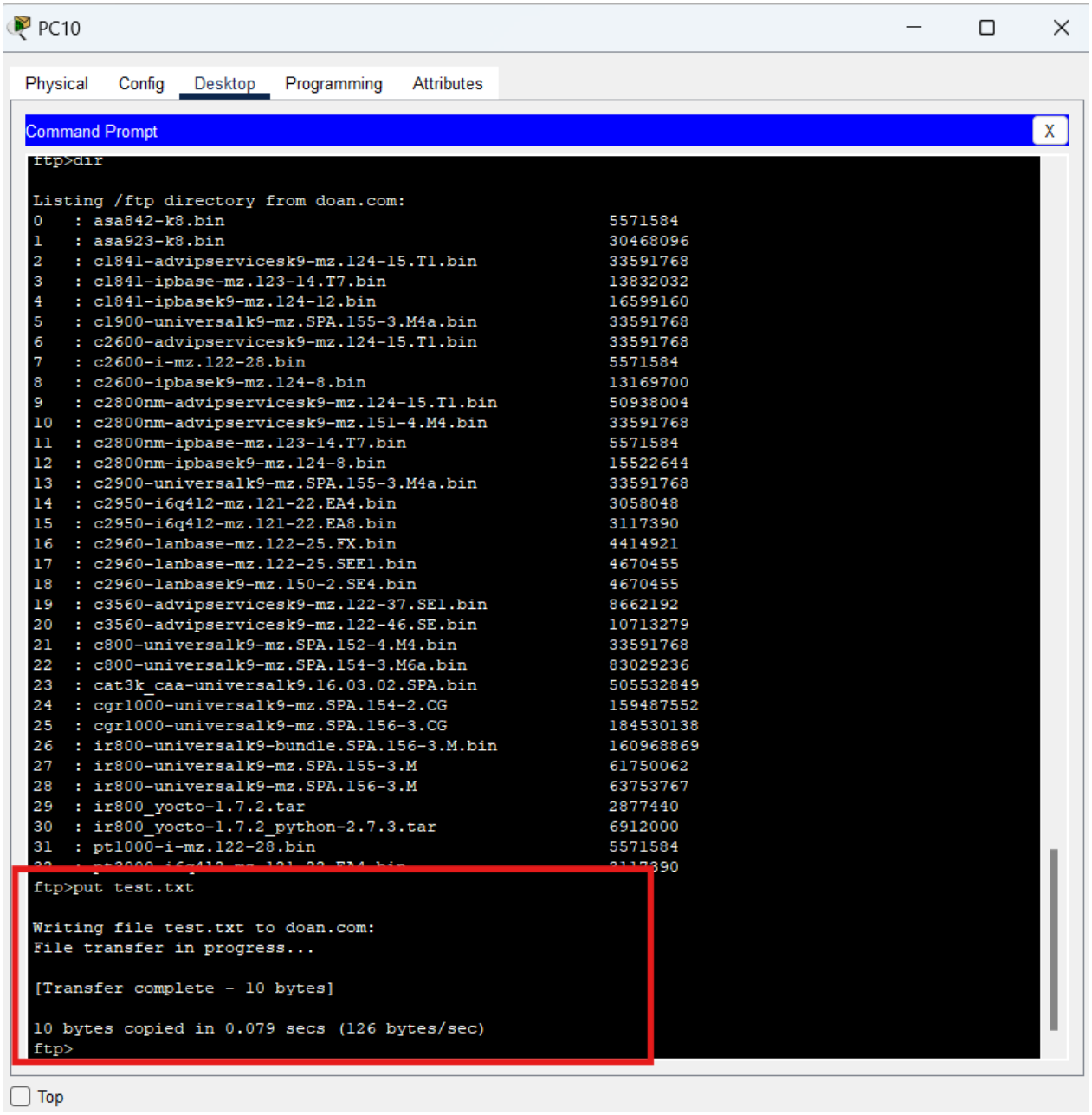
❖ Vào Command Prompt → ftp doan.com → nhập usernam và password



❖ Gõ lệnh “dir” để xem các tệp



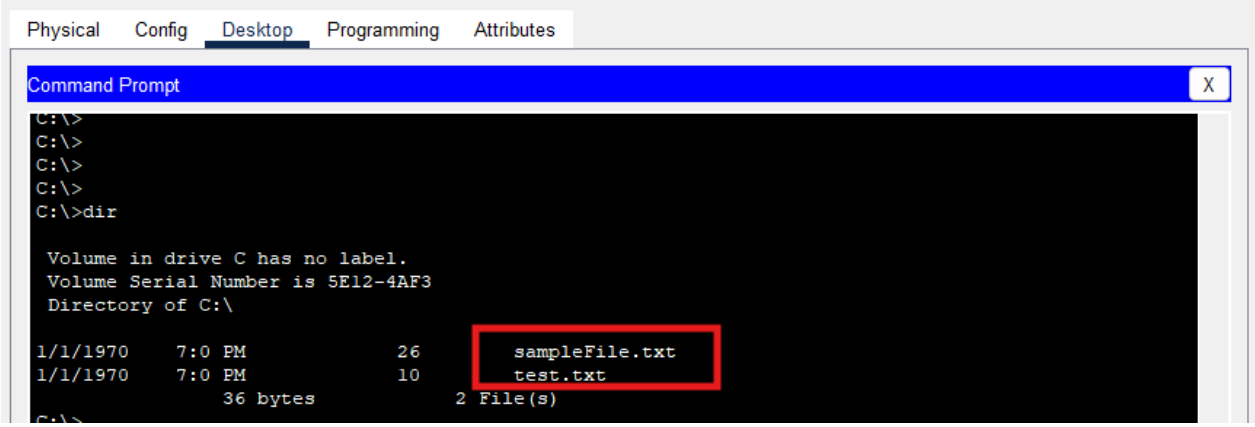
❖ Gõ lệnh put test.txt để đưa file lên server



❖ Sử dụng lệnh “get” để download file

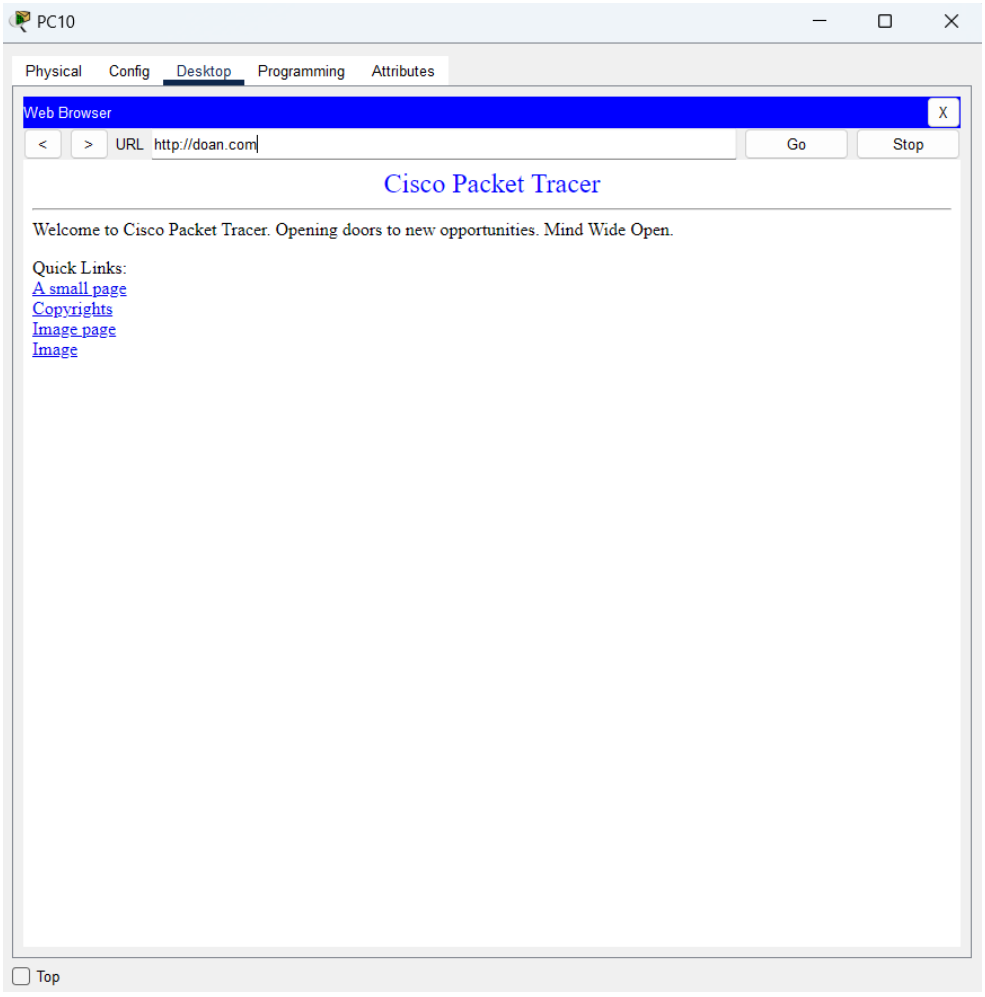
```
ftp>get test.txt

Reading file test.txt from doan.com:
File transfer in progress...

[Transfer complete - 10 bytes]

10 bytes copied in 0 secs
```

❖ Sau đó ta sẽ quit ra ngoài FTP, và dùng lệnh dir để kiểm tra xem file đã được download về nội bộ máy chưa



12. Kiểm thử dịch vụ Web Server

❖ Ở máy client ta sử dụng Web Browser để truy cập thử tên miền doan.com



Hình 60: Kiểm thử dịch vụ Web Server

CHƯƠNG IV: KẾT LUẬN

I. Kết quả đạt được

❖ Trong quá trình thực hiện đồ án "Thiết kế hệ thống mạng cho doanh nghiệp vừa và nhỏ" em đã đạt được các mục tiêu và kết quả:

- Khảo sát, phân tích được nhu cầu của đa phần các doanh nghiệp, xác định được các vấn đề phải giải quyết cho doanh nghiệp.
- Dựa trên những phân tích và nhu cầu của doanh nghiệp mà có thể thiết kế được một hệ thống mạng có thể áp dụng vào thực tiễn.

II. Một số hạn chế

❖ Mặc dù tìm hiểu và thiết kế được hệ thống mạng cho doanh nghiệp vừa và nhỏ nhưng vẫn chưa có cơ hội tiếp cận thực tế nên vẫn còn nhiều thiếu sót nổi bật trong đó:

- Cấu hình và giao thức vẫn chưa tối ưu hóa được hết hệ thống mạng cho doanh nghiệp
- Hạn chế về hệ thống bảo mật mạng
- Chưa có thiết bị dự phòng phòng cho trường hợp kết nối của router bị đứt.

III. Định hướng phát triển

❖ Để có thể phát triển được hệ thống mạng tốt hơn đầu tiên phải tìm giải pháp khắc phục những điểm còn hạn chế:

- Tối ưu hóa hệ thống mạng: theo dõi và đánh giá hệ thống mạng cũng như tối ưu hóa cấu hình để đảm bảo rằng hệ thống có thể chạy ổn định và hiệu quả.
- Tập trung vào việc xây dựng hệ thống bảo mật: tìm hiểu và triển khai các biện pháp bảo mật như hệ thống phát hiện xâm nhập (IDS), hệ thống ngăn chặn xâm nhập (IPS)
- Nâng cấp hệ thống mạng dự phòng: cấu hình dự phòng cho trường hợp router hay switch bị hỏng không thể tiếp tục thì vẫn còn router hay switch khác tiếp tục công việc mà không bị trì hoãn.

TÀI LIỆU THAM KHẢO

1. Hướng dẫn cấu hình router Cisco - QuanTriMang.com
2. CCNA LAB GUIDE – VnExperts Networking Acedemy
3. [Học MCSA 2019]
4. The Fundamentals of Networking | IBM
5. Windows Server 2022 | Microsoft
6. Tài liệu MCSA 2016
7. Giáo trình mạng máy tính Ths. Nguyên Văn Linh
8. Giáo trình Thiết kế và xây dựng mạng LAN và WAN
9. Mạng máy tính – Dương Bảo Ninh
10. Network Administration - Hamish Whittal