

BÀI TẬP LỚN

MÔN HỌC QUẢN TRỊ MẠNG

BỘ MÔN CÔNG NGHỆ THÔNG TIN

Sinh viên 1: Lã Nguyễn Minh Lượng

MSSV: K225480106044

Sinh viên 2: Dương Thị Ly

MSSV: K225480106045

Lớp: K58KTP

Ngành: Kỹ Thuật Máy Tính

Giáo viên hướng dẫn: TH.s Nghiêm Văn Tính

Ngày giao đề..... Ngày hoàn thành : 04/06/2025

Tên đề tài : Triển khai hệ thống mạng nội bộ ảo gồm 1 server và 5 client, sử dụng DHCP và DNS.....

Yêu cầu : Triển khai hệ thống mạng nội bộ ảo gồm 1 server và 5 client, sử dụng DHCP và DNS.....

GIÁO VIÊN HƯỚNG DẪN

(Ký và ghi rõ họ tên)

NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Thái Nguyên, ngày 04 tháng 06 năm 2025

GIÁO VIÊN HƯỚNG DẪN

(Ký ghi rõ họ tên)

MỤC LỤC

MỤC LỤC	3
LỜI CAM ĐOAN	4
DANH MỤC HÌNH ẢNH	5
LỜI NÓI ĐẦU	6
CHƯƠNG 1. TỔNG QUAN VỀ ĐỀ TÀI	7
1.1. Giới thiệu về dịch vụ DHCP	7
1.2. Giới thiệu về dịch vụ DNS.....	8
CHƯƠNG 2. CƠ CHẾ HOẠT ĐỘNG CỦA DHCP	13
2.1. Thủ tục phân bổ/cho thuê địa chỉ IP	13
2.2. Thủ tục gia hạn địa chỉ IP	14
2.3. Thủ tục phát hành địa chỉ IP	16
CHƯƠNG 3. QUẢN LÝ VÀ KHẮC PHỤC SỰ CỐ DHCP.....	17
3.1. Danh sách kiểm tra khắc phục sự cố.....	17
3.2. Khắc phục sự cố máy chủ DHCP.....	17
3.3. Khắc phục sự cố máy khách DHCP.....	18
3.4. Sử dụng theo dõi mạng để khắc phục sự cố DHCP.....	18
CHƯƠNG 4. THIẾT KẾ HỆ THỐNG	21
4.1. Thiết kế hệ thống.....	21
4.1.1. Giới thiệu chung về VMWARE.....	21
4.1.2. Giới thiệu window sever 2016	21
4.1.3 Giới thiệu window 10	21
4.2. Sơ đồ mạng.....	22
4.3. Mục Tiêu của hệ thống.....	20
4.4.Mối quan hệ của các dịch vụ.....	20
CHƯƠNG 5. Triển Khai Hệ Thống.....	24
5.1. Tạo máy ảo	24
5.2. Cài đặt DHCP sever	24
5.3. Cài đặt DNS sever	27
5.4. Kiểm tra hệ thống.....	28
CHƯƠNG 6. NHẬN XÉT VÀ ĐÁNH GIÁ VỀ HỆ THỐNG.....	32
6.1. Những kết quả đã đạt được	32
6.2. Tính thực tiễn của đề tài.....	32
6.3. Kỹ thuật triển khai.....	32
6.4. Những ưu điểm và hạn chế của hệ thống.....	33
KẾT LUẬN	35
TÀI LIỆU THAM KHẢO.....	36

LỜI CAM ĐOAN

Chúng tôi xin cam đoan rằng bài tập lớn ”Triển khai hệ thống mạng nội bộ ảo gồm 1 server và 5 client, sử dụng DHCP và DNS” là kết quả của quá trình nghiên cứu và thực hiện của chúng tôi. Tất cả các số liệu và tài liệu được trích dẫn trong bài tập lớn đều có nguồn gốc rõ ràng và được xác thực. Nội dung trong là duy nhất, chưa từng được công bố trong bất kỳ công trình nào trước đây. Chúng tôi xin hoàn toàn chịu trách nhiệm trước pháp luật về tính trung thực và nội dung của bài tập lớn.

Tên sinh viên

Lăng Nguyễn Minh Lượng

Dương Thị Ly

DANH MỤC HÌNH ẢNH

Hình 2.1. Quy trình phân bổ/cho thuê địa chỉ IP sử dụng DHCP.....	13
Hình 2.2. Quy trình gia hạn thuê địa chỉ IP sử dụng DHCP.....	15
Hình 2.3. Quy trình giải phóng địa chỉ IP bằng DHCP	16
Hình 3.1. thao tác dừng bắt gói tin trong Wireshark	19
Hình 3.2. Vai trò của Transaction ID trong việc theo dõi và phân tích quá trình cấp phát địa chỉ IP qua DHCP	19
Hình 4.1. Sơ đồ mạng.....	22
Hình 5.1. Cài đặt DHCP.....	24
Hình 5.2. Chọn cửa sổ DHCP	25
Hình 5.3. Setup giải địa chỉ cấp phát	25
Hình 5.4. Cấu hình cho DHCP Server cung cấp thông tin DNS đến các máy client khi cấp phát IP.....	26
Hình 5.5. Cài đặt DNS	27
Hình 5.6. Chọn cửa sổ DNS.....	27
Hình 5.7. Tạo mới một DNS zone	28
Hình 5.8. Client 1 đã được cấp ip động từ server	29
Hình 5.9. Client 2 đã được cấp ip động từ server	29
Hình 5.10. Client 3 đã được cấp ip động từ server	30
Hình 5.11. Client 4 đã được cấp ip động từ server	30
Hình 5.12. Client 5 đã được cấp ip động từ server	31

LỜI NÓI ĐẦU

Trong thời đại công nghệ thông tin phát triển mạnh mẽ, việc xây dựng và quản trị một hệ thống mạng ổn định, hiệu quả là yếu tố then chốt đối với mọi tổ chức và doanh nghiệp. Môn học *Quản trị mạng* không chỉ trang bị kiến thức lý thuyết mà còn tạo cơ hội cho sinh viên tiếp cận thực tế qua các đề tài triển khai mô hình mạng cụ thể.

Với mục tiêu đó, em đã chọn đề tài **“Triển khai hệ thống mạng gồm 5 máy trạm (client) và 1 máy chủ (server) sử dụng dịch vụ DHCP và DNS”**. Đây là mô hình cơ bản nhưng rất thiết thực, giúp em hiểu rõ hơn về cách một mạng nội bộ vận hành, cũng như vai trò quan trọng của các dịch vụ như **DHCP** (tự động cấp phát địa chỉ IP) và **DNS** (hệ thống phân giải tên miền).

Trong quá trình thực hiện, em đã tìm hiểu và áp dụng các bước triển khai như: cài đặt hệ điều hành cho máy chủ, cấu hình dịch vụ DHCP và DNS, kết nối và kiểm tra tính năng giữa các client trong mạng. Thông qua đó, em đã củng cố được kỹ năng cấu hình và xử lý sự cố mạng – những kỹ năng cần thiết cho công việc sau này.

Em xin chân thành cảm ơn thầy Nghiêm Văn Tính đã tận tình hướng dẫn và hỗ trợ em trong suốt quá trình thực hiện đề tài. Mặc dù đã cố gắng hoàn thiện bài báo cáo một cách tốt nhất, nhưng do giới hạn về thời gian và kinh nghiệm, bài làm không tránh khỏi những thiếu sót. Em rất mong nhận được sự góp ý từ thầy/cô để em có thể cải thiện và học hỏi thêm.

CHƯƠNG 1. TỔNG QUAN VỀ ĐỀ TÀI

1.1. Giới thiệu về dịch vụ DHCP

a. Máy chủ DHCP là gì?

- **Máy chủ DHCP (DHCP Server)** là một máy chủ mạng có chức năng tự động cung cấp và gán địa chỉ IP, cổng mặc định (default gateway) và các thông số mạng khác cho các thiết bị đầu cuối (client). Nó hoạt động dựa trên giao thức tiêu chuẩn gọi là DHCP (Dynamic Host Configuration Protocol) – giao thức cấu hình động máy chủ, để phản hồi các truy vấn quảng bá (broadcast) từ các thiết bị client.

b. Tại sao chúng ta sử dụng DHCP?

- DHCP cho phép quản trị viên mạng quản lý tập trung nhóm địa chỉ IP giữa các máy chủ và tự động hóa việc chỉ định địa chỉ IP trong mạng.
- DHCP giúp bạn giảm số lượng địa chỉ IP cần thiết trên mạng khi bạn sử dụng nó để quản lý nhóm địa chỉ IP giữa các máy chủ. DHCP thực hiện điều này bằng cách cho thuê địa chỉ IP cho máy chủ trong một khoảng thời gian giới hạn, cho phép máy chủ DHCP chia sẻ một số lượng địa chỉ IP giới hạn.
- DHCP giảm thiểu chi phí cần thiết để thêm máy khách vào mạng bằng cách cung cấp thiết lập tập trung dựa trên máy chủ, nghĩa là bạn không phải tạo và duy trì thủ công việc chỉ định địa chỉ IP cho máy khách.
- DHCP cung cấp cơ sở dữ liệu trung tâm về các thiết bị được kết nối với mạng và loại bỏ việc phân bổ tài nguyên trùng lặp.
- DHCP tự động gán tham số mạng cho các thiết bị mạng. Ngay cả trong các mạng nhỏ, DHCP vẫn hữu ích vì nó giúp dễ dàng thêm máy mới vào mạng.
- DHCP cung cấp thông tin cấu hình khác, đặc biệt là địa chỉ IP của bộ phân giải Hệ thống tên miền (DNS) lưu trữ cục bộ, máy chủ khởi động mạng hoặc các máy chủ dịch vụ khác ngoài địa chỉ IP cho máy khách.
- DHCP trên thiết bị Junos OS có thể tự động nâng cấp phần mềm trên hệ thống máy khách.

c. Các thành phần của DHCP

- **Máy chủ DHCP:** Máy chủ DHCP là máy chủ lưu trữ Địa chỉ IP và các thông tin khác liên quan đến cấu hình.
- **DHCP Client:** Là thiết bị nhận thông tin cấu hình từ máy chủ. Có thể là điện thoại di động, máy tính xách tay, máy tính hoặc bất kỳ thiết bị điện tử nào khác cần kết nối.
- **Chuyển tiếp DHCP:** Chuyển tiếp DHCP về cơ bản hoạt động như một kênh truyền thông giữa Máy khách và Máy chủ DHCP.
- **Nhóm địa chỉ IP:** Đây là nhóm hoặc vùng chứa Địa chỉ IP do Máy chủ DHCP sở hữu. Nó có một phạm vi địa chỉ có thể được phân bổ cho các thiết bị.
- **Mạng con:** Mạng con là những phần nhỏ hơn của mạng IP được phân vùng để kiểm soát mạng.
- **Lease:** Đơn giản là thời hạn thông tin nhận được từ máy chủ có hiệu lực, trong trường hợp thời hạn thuê hết hạn, người thuê phải chuyển nhượng lại hợp đồng thuê.
- **Máy chủ DNS:** Máy chủ DHCP cũng có thể cung cấp thông tin máy chủ DNS (Hệ thống tên miền) cho máy khách DHCP, cho phép chúng phân giải tên miền thành địa chỉ IP.
- **Cổng mặc định:** Máy chủ DHCP cũng có thể cung cấp thông tin về cổng mặc định, đây là thiết bị mà các gói tin được gửi đến khi đích đến nằm ngoài mạng cục bộ.
- **Tùy chọn:** Máy chủ DHCP có thể cung cấp các tùy chọn cấu hình bổ sung cho máy khách, chẳng hạn như mặt nạ mạng con, tên miền và thông tin máy chủ thời gian.
- **Gia hạn:** Máy khách DHCP có thể yêu cầu gia hạn hợp đồng thuê trước khi hết hạn để đảm bảo rằng họ tiếp tục có địa chỉ IP và thông tin cấu hình hợp lệ.
- **Chuyển đổi dự phòng:** Máy chủ DHCP có thể được cấu hình để chuyển đổi dự phòng, trong đó hai máy chủ hoạt động cùng nhau để cung cấp khả năng dự phòng và đảm bảo rằng máy khách luôn có thể nhận được địa chỉ IP và thông tin cấu hình, ngay cả khi một máy chủ ngừng hoạt động.
- **Cập nhật động:** Máy chủ DHCP cũng có thể được cấu hình để cập nhật động các bản ghi DNS với địa chỉ IP của máy khách DHCP, cho phép quản lý tài nguyên mạng dễ dàng hơn.
- **Nhật ký kiểm tra:** Máy chủ DHCP có thể lưu giữ nhật ký kiểm tra của tất cả các giao dịch DHCP, cung cấp cho người quản trị khả năng hiển thị thiết bị nào đang sử dụng địa chỉ IP nào và khi nào hợp đồng thuê được cấp hoặc gia hạn.

d. Hoạt động của DHCP

Tác nhân chuyển tiếp DHCP nằm giữa máy khách DHCP và máy chủ DHCP và chuyển tiếp các tin nhắn DHCP giữa máy chủ và máy khách như sau:

- Máy khách DHCP gửi một gói khám phá để tìm máy chủ DHCP trong mạng để lấy các thông số cấu hình cho người đăng ký (hoặc máy khách DHCP), bao gồm cả địa chỉ IP.
- DHCP relay agent nhận gói discover và chuyển tiếp các bản sao đến mỗi máy chủ DHCP. Sau đó, DHCP relay agent tạo một mục trong bảng máy khách nội bộ của nó để theo dõi trạng thái của máy khách.
- Để đáp lại việc nhận được gói khám phá, mỗi máy chủ DHCP gửi một gói đề nghị đến máy khách. Tác nhân chuyển tiếp DHCP nhận các gói đề nghị và chuyển tiếp chúng đến máy khách DHCP.
- Khi nhận được các gói tin cung cấp, máy khách DHCP sẽ chọn máy chủ DHCP để lấy thông tin cấu hình. Thông thường, máy khách sẽ chọn máy chủ cung cấp thời gian thuê dài nhất trên địa chỉ IP.
- Máy khách DHCP gửi một gói yêu cầu chỉ định máy chủ DHCP để lấy thông tin cấu hình.
- Tác nhân chuyển tiếp DHCP nhận gói yêu cầu và chuyển tiếp các bản sao tới mỗi máy chủ DHCP.
- Máy chủ DHCP được máy khách yêu cầu sẽ gửi một gói tin xác nhận (ACK) có chứa các tham số cấu hình của máy khách.
- Bộ chuyển tiếp DHCP nhận gói tin ACK và chuyển tiếp nó tới máy khách.
- Máy khách DHCP nhận gói tin ACK và lưu trữ thông tin cấu hình.
- Nếu được cấu hình để thực hiện như vậy, tác nhân chuyển tiếp DHCP sẽ cài đặt tuyến máy chủ và mục Giao thức phân giải địa chỉ (ARP) cho máy khách này.
- Sau khi thiết lập hợp đồng thuê ban đầu trên địa chỉ IP, máy khách DHCP và máy chủ DHCP sử dụng truyền đơn hướng để thương lượng gia hạn hoặc giải phóng hợp đồng thuê. Tác nhân chuyển tiếp DHCP "snoop" trên tất cả các gói đơn hướng giữa máy khách và máy chủ đi qua bộ định tuyến (hoặc bộ chuyển mạch) để xác định thời điểm hợp đồng thuê cho máy khách này đã hết hạn hoặc được giải phóng. Quá trình này được gọi là che giấu hợp đồng thuê hoặc snoop thụ động.

e. Những cân nhắc về bảo mật khi sử dụng DHCP

- **Địa chỉ IP giới hạn** : Máy chủ DHCP chỉ có thể cung cấp một số lượng địa chỉ IP nhất định. Điều này có nghĩa là kẻ tấn công có thể làm tràn ngập máy chủ bằng các yêu cầu, khiến các thiết bị cần thiết mất kết nối.
- **Máy chủ DHCP giả** : Kẻ tấn công có thể thiết lập máy chủ DHCP giả để cung cấp địa chỉ IP giả cho các thiết bị trong mạng của bạn.
- **Truy cập DNS** : Khi người dùng nhận được địa chỉ IP từ DHCP, họ cũng nhận được thông tin chi tiết về máy chủ DNS. Điều này có khả năng cho phép họ truy cập nhiều dữ liệu hơn mức cần thiết. Điều quan trọng là phải hạn chế quyền truy cập mạng, sử dụng tường lửa và kết nối an toàn với VPN để bảo vệ chống lại điều này.

f. Những hạn chế khi dùng router/switch làm máy chủ DHCP

- Tiêu tốn tài nguyên của thiết bị mạng, do các gói DHCP được xử lý bằng phần mềm, không được tăng tốc phần cứng như các gói tin chuyên tiếp thông thường.
- Không hỗ trợ DNS động (Dynamic DNS) – thiết bị không thể tạo bản ghi DNS thay cho client dựa trên địa chỉ IP đã cấp phát.
- Không thể quản lý tập trung các scope DHCP hoặc xem toàn bộ danh sách các client đã được cấp IP trên nhiều thiết bị. Quản trị viên phải đăng nhập từng switch/router để kiểm tra.
- Không có tính năng dự phòng (redundancy) hoặc khả năng chịu lỗi cao (high availability). Nếu thiết bị DHCP hiện tại bị lỗi, các client có thể mất kết nối.
- Cấu hình DHCP trên router/switch thường phức tạp và hạn chế, không trực quan như máy chủ chuyên dụng.
- Không tích hợp được với hệ thống quản lý địa chỉ IP (IPAM) – thiếu khả năng theo dõi, phân tích, bảo mật và giám sát mạng.

1.2. Giới thiệu về dịch vụ DNS

a. DNS là gì?

- DNS (Domain Name System) là hệ thống phân giải tên miền – có chức năng **chuyển đổi tên miền (hostname)** thành **địa chỉ IP** tương ứng để các thiết bị trong mạng có thể tìm và giao tiếp với nhau.
- Trong mạng máy tính, các thiết bị chỉ hiểu và giao tiếp thông qua địa chỉ IP. Tuy nhiên, việc ghi nhớ IP là rất khó khăn, vì vậy DNS giúp người dùng sử dụng tên dễ nhớ hơn như: K58KTP_QTM.tnut thay vì 192.168.220.130

b. Tại sao cần DNS trong hệ thống này?

- Hệ thống của em có **1 Server và 5 Client**, nếu không dùng DNS thì mọi kết nối đều phải nhớ IP – rất bất tiện và dễ sai sót.
- DNS cho phép:
 - Client **truy cập dịch vụ trên Server bằng tên thay vì IP** (ví dụ: K58KTP_QTM.tnut)
 - Hệ thống dễ mở rộng và quản lý hơn trong tương lai.
 - Hỗ trợ các dịch vụ phụ thuộc tên miền như **Web Server, File Server, Active Directory**, v.v.

c. DNS hoạt động thế nào trong hệ thống

- **DNS Server được cài trên chính máy Server** (Windows Server 2016).
- Khi **Client cần truy cập tài nguyên trên Server bằng tên miền**, nó sẽ gửi truy vấn DNS đến DNS Server để phân giải tên đó thành IP.
- DNS trả về địa chỉ IP tương ứng, giúp Client kết nối được với Server.

d. Vai trò cụ thể của DNS trong hệ thống

Vai trò	Mô tả
Phân giải tên miền nội bộ	K58KTP_QTM.tnut ->192.168.220.130
Hỗ trợ DHCP cấp DNS tự động	Khi Client nhận IP từ DHCP, nó cũng được cấp luôn địa chỉ DNS (chính là IP của DNS Server)
Hỗ trợ các dịch vụ dựa vào tên miền	Ví dụ nếu sau này em triển khai Web Server hoặc chia sẻ file thì DNS là bắt buộc
Truy cập tài nguyên dễ dàng hơn	Người dùng chỉ cần nhớ tên server thay vì IP (gõ \\ K58KTP_QTM.tnut)

e. Quy trình phân giải DNS nội bộ

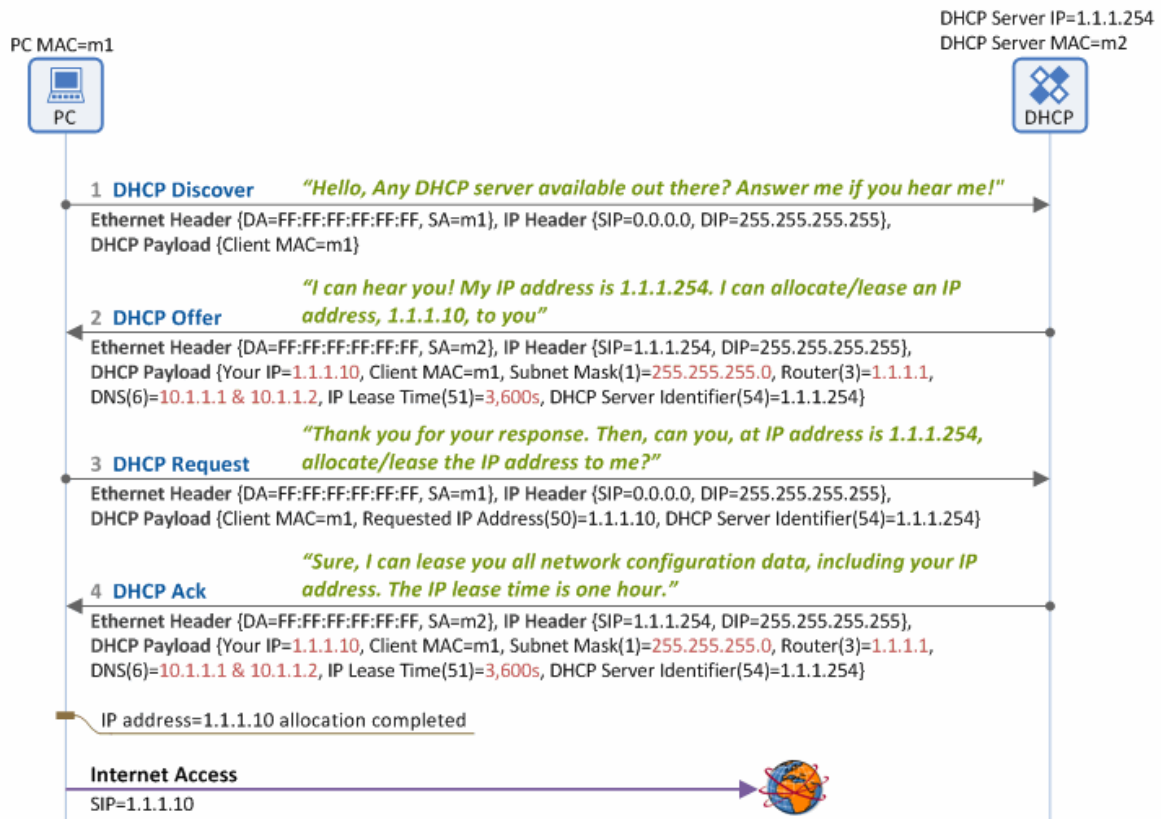
- Client gõ: \\ K58KTP_QTM.tnut
- Hệ thống kiểm tra cache DNS cục bộ (nếu có).
- Nếu không có, Client gửi truy vấn đến DNS Server (được cấp bởi DHCP).
- DNS Server tìm bản ghi A (hoặc PTR nếu reverse).
- Trả lại IP tương ứng: 192.168.220.130.
- Client dùng IP đó để kết nối tới Server.

f. Tại sao nên tách riêng DNS ra thay vì dùng IP tĩnh mãi mãi?

- Dễ mở rộng hệ thống: thêm nhiều server và client mà không cần nhớ IP.
- Dễ cấu hình dịch vụ mạng nâng cao: như Active Directory, Web Server...
- Thay đổi IP không ảnh hưởng đến người dùng: vì vẫn giữ nguyên tên miền.

CHƯƠNG 2. CƠ CHẾ HOẠT ĐỘNG CỦA DHCP

2.1. Thủ tục phân bổ/cho thuê địa chỉ IP



Hình 2.1. Quy trình phân bổ/cho thuê địa chỉ IP sử dụng DHCP

→ Khám phá DHCP

Khi máy khách (PC) khởi động, máy khách sẽ phát thông báo DHCP Discover qua mạng Ethernet để xác định vị trí tất cả các máy chủ DHCP khả dụng trên cùng một mạng con (bằng cách đặt địa chỉ MAC đích trong tiêu đề Ethernet là Broadcast MAC=FF:FF:FF:FF:FF:FF), đến được tất cả các máy chủ DHCP trên cùng một mạng con.

→ Đề nghị DHCP

Khi máy chủ DHCP nhận được tin nhắn DHCP Discover từ máy khách, nó cũng phát tin nhắn DHCP Offer qua mạng Ethernet (vì địa chỉ IP của máy khách vẫn chưa được phân bổ), thông báo cho máy khách rằng nó khả dụng. Tin nhắn này chứa thông tin mạng, chẳng hạn như địa chỉ IP của máy khách, mặt nạ mạng con, địa chỉ IP của công mặc định, địa chỉ IP DNS, thời gian thuê IP và địa chỉ IP của máy chủ DHCP. Tin nhắn DHCP Offer được phát sẽ được gửi đến tất cả máy khách trên cùng một mạng con, bao gồm cả máy khách đã gửi tin nhắn DHCP Discover.

→ **Yêu cầu DHCP**

Máy khách, sau khi nhận được thông báo DHCP Offer, nhận ra có một máy chủ DHCP khả dụng trên cùng một mạng con. Sau đó, nó phát thông báo DHCP Request đến máy chủ qua mạng Ethernet, yêu cầu dữ liệu cấu hình mạng bao gồm địa chỉ IP cho chính nó. Nếu có nhiều hơn một máy chủ DHCP phản hồi trên cùng một mạng con và do đó máy khách nhận được nhiều thông báo DHCP Offer, nó sẽ chọn một trong các máy chủ DHCP và nhập địa chỉ IP của máy chủ DHCP đã chọn vào trường DHCP Server Identifier (tùy chọn 54) của thông báo DHCP Request. Sau đó, nó thông báo cho tất cả các máy chủ DHCP trên mạng con về lựa chọn đó bằng cách phát thông báo DHCP Request. Thông thường, tất cả các máy chủ DHCP đều lưu trữ dữ liệu cấu hình mạng bên trong (tức là địa chỉ IP cho máy khách và thông tin khác) khi chúng gửi thông báo DHCP Offer. Vì vậy, máy khách phát thông báo DHCP Request đến tất cả các máy chủ DHCP, để những máy chủ không được chọn cũng có thể nhận được thông báo và xóa dữ liệu cấu hình mạng đã lưu trữ khỏi bộ nhớ của chúng.

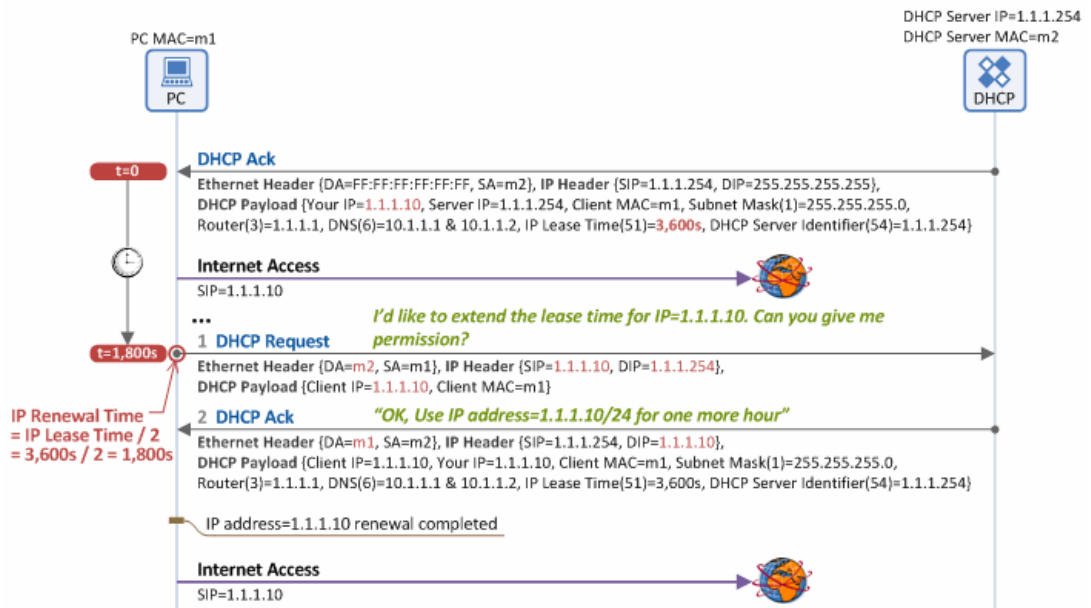
→ **Xác nhận DHCP**

Máy chủ DHCP nhận được thông báo Yêu cầu DHCP từ máy khách sẽ kiểm tra xem địa chỉ IP hiển thị trong trường DHCP Server Identifier (tùy chọn 54) có khớp với địa chỉ IP của máy chủ đó không. Nếu khớp, máy chủ sẽ phát thông báo DHCP Ack để đảm bảo máy khách có thể nhận được thông báo (Lưu ý: máy khách CHƯA được cấp địa chỉ IP).

Vào thời điểm này, máy chủ DHCP chuyển tất cả dữ liệu cấu hình mạng bao gồm địa chỉ IP của máy khách – cùng dữ liệu được gửi cùng với thông báo DHCP Offer – đến máy khách. Sau đó, máy khách cấu hình giao diện mạng bằng dữ liệu được chuyển, cuối cùng kết nối với Internet. Dữ liệu cấu hình mạng thông thường bao gồm:

- Địa chỉ IP
- Mặt nạ mạng con
- Địa chỉ IP cổng mặc định
- Địa chỉ IP của máy chủ DNS
- Thời gian thuê (trong thời gian đó máy khách có thể sử dụng địa chỉ IP được phân bổ/thuê bởi máy chủ DHCP)

2.2. Thủ tục gia hạn địa chỉ IP



Hình 2.2. Quy trình gia hạn thuê địa chỉ IP sử dụng DHCP

→ Yêu cầu DHCP

Trong Hình 3, thời gian thuê được đưa ra là 1 giờ. Khi một nửa thời gian đã trôi qua (tức là 1.800 giây/30 phút trong Hình 3), máy khách sẽ gửi tin nhắn Yêu cầu DHCP đến máy chủ DHCP để gia hạn thời gian thuê (Lưu ý: Trong trường hợp gia hạn IP, không cần quy trình Khám phá/Đề nghị DHCP). Không giống như trong quy trình phân bổ/cho thuê địa chỉ IP, máy khách không phát tin nhắn Yêu cầu DHCP (MẠC Đích = FF: FF: FF: FF: FF: FF, IP Đích = 255.255.255.255), nhưng phát đơn hướng (MAC Đích = DHCP Server MAC (m2), IP Đích = DHCP Server IP (1.1.1.254)). Điều đó là do máy chủ DHCP và máy khách đã biết địa chỉ IP của nhau. Thông báo Yêu cầu DHCP để gia hạn địa chỉ IP phải bao gồm địa chỉ IP của máy khách yêu cầu gia hạn trong trường "Địa chỉ IP của máy khách (ciaddr)", nhưng phải loại trừ các trường Địa chỉ IP được yêu cầu (tùy chọn 50) và Mã định danh máy chủ DHCP (tùy chọn 54).

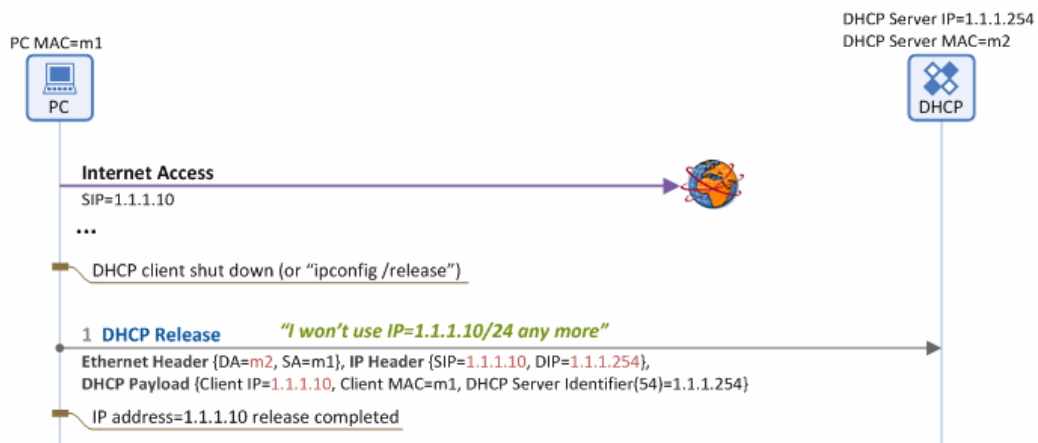
→ Xác nhận DHCP

Khi chấp nhận tin nhắn DHCP Request (để gia hạn địa chỉ IP) nhận được từ máy khách, máy chủ DHCP cũng phát đơn hướng và không phát tin nhắn DHCP Ack (MẠC đích=MẠC của máy tính (m1), IP đích=MẠC IP của máy tính (1.1.1.10)), bao gồm dữ liệu cấu hình mạng như địa chỉ IP của máy khách, mặt nạ mạng con, địa chỉ IP của cổng mặc định, địa chỉ IP DNS và thời gian thuê, cho máy khách. Sau khi quá trình này hoàn tất, máy khách có thể giữ địa

chỉ IP hiện tại của mình trong thời gian thuê mở rộng như được chỉ định trong tin nhắn DHCP Ack.

2.3. Thủ tục phát hành địa chỉ IP

Khi một máy khách tắt hẳn, lệnh `1` hoặc `'ipconfig/release'` được nhập vào cửa sổ lệnh DOS của Windows, máy khách sẽ gửi một thông báo Yêu cầu DHCP đến máy chủ DHCP để trả về địa chỉ IP được phân bổ của nó, như trong Hình 4. Sau đó, nó giải phóng dữ liệu cấu hình mạng (tức là địa chỉ IP của máy khách, mặt nạ mạng con, địa chỉ IP cổng mặc định, địa chỉ IP DNS, v.v.), do đó không còn có thể truy cập Internet nữa.



Hình 2.3. Quy trình giải phóng địa chỉ IP bằng DHCP

→ Phát hành DHCP

Nếu máy khách không cần địa chỉ IP được phân bổ nữa, nó sẽ phát một thông báo DHCP Release (Destination MAC=DHCP Server MAC (m2), Destination IP=DHCP Server IP (1.1.1.254)) đến máy chủ DHCP. Sau đó, máy chủ sẽ giải phóng địa chỉ IP của máy khách (1.1.1.10) được liệt kê trong trường Client IP của thông báo đã nhận.

CHƯƠNG 3. QUẢN LÝ VÀ KHẮC PHỤC SỰ CỐ DHCP

3.1. Danh sách kiểm tra khắc phục sự cố

Trước khi bắt đầu khắc phục sự cố, hãy kiểm tra các mục sau:

- Vấn đề bắt đầu từ khi nào?
- Có thông báo lỗi nào không?
- Máy chủ DHCP có hoạt động trước đây không, hay chưa bao giờ hoạt động? Nếu đã hoạt động trước đây, có bất kỳ thay đổi nào trước khi sự cố xảy ra không. Ví dụ, đã cài đặt bản cập nhật chưa? Có thay đổi nào đối với cơ sở hạ tầng không?
- Vấn đề này dai dẳng hay không liên tục? Nếu không liên tục, lần cuối cùng nó xảy ra là khi nào?
- Lỗi cho thuê địa chỉ xảy ra với tất cả máy khách hay chỉ với một số máy khách cụ thể, chẳng hạn như mạng con phạm vi đơn?
- Có máy khách nào trên cùng mạng con với máy chủ DHCP không?
- Nếu máy khách nằm trên cùng một mạng con, họ có thể lấy được địa chỉ IP không?
- Nếu máy khách không nằm trên cùng một mạng con, thì bộ định tuyến hoặc bộ chuyển mạch VLAN có được cấu hình đúng để có tác nhân chuyển tiếp DHCP (còn gọi là Trình trợ giúp IP) không?
- Máy chủ DHCP có hoạt động độc lập hay được cấu hình để có tính khả dụng cao, chẳng hạn như phạm vi chia tách hoặc DHCP Failover?
- Kiểm tra các thiết bị trung gian để tìm các tính năng như VRRP/HSRP, Kiểm tra ARP động hoặc DHCP snooping có thể gây ra sự cố.

3.2. Khắc phục sự cố máy chủ DHCP

Đối với máy chủ DHCP, hãy kiểm tra các thiết bị và cài đặt sau:

- Dịch vụ máy chủ DHCP đã được khởi động và chạy. Để kiểm tra cài đặt này, hãy chạy `net start` lệnh và tìm **DHCP Server**.
- Máy chủ DHCP đã được cấp phép. Xem Windows DHCP Server Authorization trong Kịch bản tham gia miền.
- Xác minh rằng các hợp đồng cho thuê địa chỉ IP có sẵn trong phạm vi máy chủ DHCP cho mạng con mà máy khách DHCP đang sử dụng. Để thực hiện việc này, hãy xem số liệu thống kê cho phạm vi phù hợp trong bảng điều khiển quản lý máy chủ DHCP.
- Kiểm tra xem có tìm thấy danh sách BAD_ADDRESS nào trong phần Cho thuê địa chỉ không.
- Kiểm tra xem có thiết bị nào trên mạng có địa chỉ IP tĩnh chưa bị loại trừ khỏi phạm vi DHCP không.
- Xác minh rằng địa chỉ IP mà máy chủ DHCP được liên kết nằm trong mạng con của phạm vi mà địa chỉ IP phải được cho thuê. Điều này áp dụng trong trường hợp không có tác nhân chuyển tiếp nào khả dụng.

Để thực hiện việc này, hãy chạy lệnh ghép ngắn `Get-`

`DhcpServerv4BindingOr Get-DhcpServerv6Binding`.

- Xác minh rằng chỉ có máy chủ DHCP đang lắng nghe trên cổng UDP 67 và 68. Không có quy trình hoặc dịch vụ nào khác (như WDS hoặc PXE) được chiếm các cổng này. Để thực hiện việc này, hãy chạy `netstat -anbl`.
- Nếu bạn đang xử lý môi trường triển khai IPsec, hãy xác minh rằng miễn trừ IPsec của máy chủ DHCP đã được thêm vào.
- Xác minh rằng địa chỉ IP của tác nhân chuyển tiếp có thể được ping từ máy chủ DHCP.
- Liệt kê và kiểm tra các chính sách và bộ lọc DHCP đã cấu hình.

3.3. Khắc phục sự cố máy khách DHCP

Đối với máy khách DHCP, hãy kiểm tra các thiết bị và cài đặt sau:

- Cáp đã được kết nối và hoạt động.
- Lọc MAC được bật trên các thiết bị chuyển mạch mà máy khách được kết nối.
- Bộ điều hợp mạng đã được bật.
- Trình điều khiển bộ điều hợp mạng chính xác đã được cài đặt và cập nhật.
- Dịch vụ DHCP Client đã được khởi động và chạy. Để kiểm tra, hãy chạy lệnh `net start` và tìm DHCP Client.
- Không có tường lửa nào chặn cổng 67 và 68 UDP trên máy khách.

3.4. Sử dụng theo dõi mạng để khắc phục sự cố DHCP

- Sau khi xác nhận cài đặt trên cả máy khách và máy chủ DHCP có thể sử dụng Wireshark để kiểm tra xem quy trình DHCP DORA đã hoàn tất thành công hay chưa hoặc có gói tin nào bị loại bỏ không cho máy khách DHCP nhận địa chỉ IP từ máy chủ hay không.

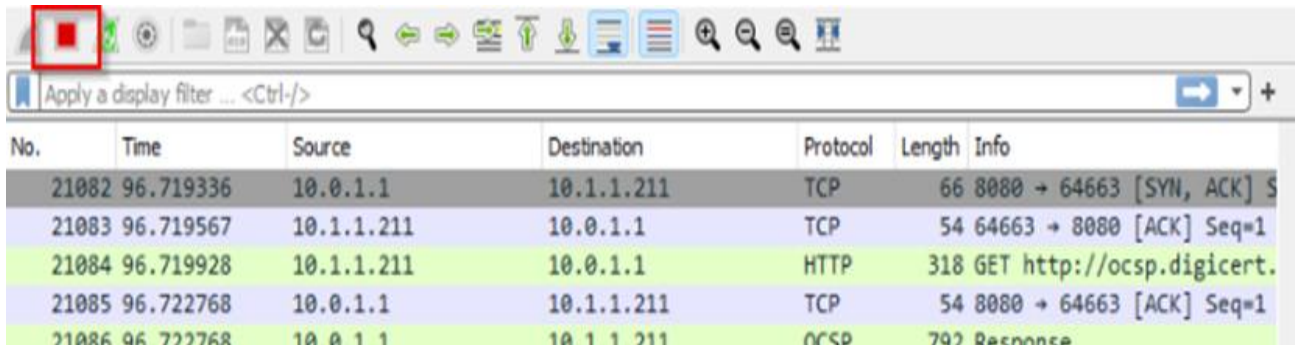
- Các bước để thu thập dấu vết mạng:

Để khắc phục sự cố DHCP bằng cách sử dụng dấu vết mạng, hãy làm theo các bước sau:

→ Cài đặt Wireshark trên cả máy khách DHCP bị ảnh hưởng và máy chủ DHCP.

→ Chạy Wireshark với tư cách quản trị viên trên cả máy khách và máy chủ.

- Chọn giao diện mạng được sử dụng cho DHCP trên cả hai thiết bị bằng cách nhấp đúp vào chúng trong Wireshark.
- Bắt đầu bắt gói tin bằng Wireshark trên cả máy khách và máy chủ.
- Tái tạo sự cố. Kích hoạt sự cố DHCP (ví dụ: chạy `ipconfig /renew` trên máy khách). Chờ cho đến khi xảy ra tình huống lỗi.
- Dừng việc bắt gói tin trên cả hai thiết bị bằng nút màu đỏ trong Wireshark.



Hình 3.1. thao tác dừng bắt gói tin trong Wireshark

- Lưu các gói tin đã chụp vào một vị trí đã chỉ định bằng cách chọn **Tập > Lưu dưới dạng**.
- Áp dụng bộ lọc DHCP để xem các giao dịch DHCP:
 - Khi chụp máy khách, hãy áp dụng bộ lọc hiển thị cho "dhcp".
 - Trên máy chủ capture, sử dụng bộ lọc "dhcp.id == <Transaction ID>" để theo dõi giao dịch máy khách cụ thể. Bạn có thể lấy ID giao dịch từ bản capture phía máy khách và áp dụng nó trong bộ lọc trên bản capture phía máy chủ.

No.	Time	Source	Destination	Protocol	Length	Info
5	2.240980	10.1.1.211	10.1.1.1	DHCP	342	DHCP Release - Transaction ID 0xeeb0daf2
43	6.286194	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x63b5ab5f
44	6.287920	10.1.1.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x63b5ab5f
45	6.289543	0.0.0.0	255.255.255.255	DHCP	367	DHCP Request - Transaction ID 0x63b5ab5f
46	6.290808	10.1.1.1	255.255.255.255	DHCP	344	DHCP ACK - Transaction ID 0x63b5ab5f

Hình 3.2. Vai trò của **Transaction ID** trong việc theo dõi và phân tích quá trình cấp phát địa chỉ IP qua DHCP

- Phân tích giao dịch DHCP:
 - Kiểm tra việc bắt giữ phía máy khách đối với tất cả bốn gói DHCP (DISCOVER, OFFER, REQUEST, ACK). Nếu tất cả đều có, thì quá trình DORA có khả năng thành công.
 - Nếu bất kỳ gói tin nào bị thiếu (ví dụ: chỉ có các gói tin DISCOVER hiển thị), điều này cho thấy khả năng mất gói tin.

→ Xác định tình trạng mất mạng. Tìm kiếm các chỉ số sau về tình trạng mất mạng:

- Việc chụp máy khách sẽ hiển thị các gói DISCOVER, nhưng việc chụp máy chủ thì không.
- Việc chụp máy khách hiển thị các gói DISCOVER và máy chủ hiển thị OFFER đã gửi nhưng không thấy OFFER trên máy khách.
- Khi chụp máy khách sẽ hiển thị DISCOVER, OFFER và REQUEST, nhưng máy chủ chỉ hiển thị DISCOVER và OFFER.
- Quá trình chụp máy khách hiển thị DISCOVER, OFFER và REQUEST, nhưng máy chủ hiển thị cả bốn gói tin đã hoàn thành (DISCOVER, OFFER, REQUEST, ACK) mà không thấy ACK nào trên máy khách.

→ Sau khi xác nhận sự cố rơi, hãy liên hệ với nhóm mạng để điều tra và giải quyết sự cố rơi.

CHƯƠNG 4. THIẾT KẾ HỆ THỐNG

4.1. Giới thiệu Về phần mềm mô phỏng

4.1.1. Giới thiệu chung về VMWARE

VMware là phần mềm ảo hóa cho phép tạo và quản lý nhiều máy ảo trên cùng một máy tính vật lý. Người dùng có thể chạy song song nhiều hệ điều hành khác nhau như Windows, Linux hoặc macOS mà không cần cài đặt trực tiếp. Các sản phẩm phổ biến như VMware Workstation, Fusion và ESXi hỗ trợ cả cá nhân lẫn doanh nghiệp. VMware giúp tiết kiệm chi phí phần cứng, tăng tính bảo mật, dễ dàng thử nghiệm phần mềm và hỗ trợ hiệu quả trong học tập, nghiên cứu cũng như triển khai hệ thống mạng nội bộ ảo.

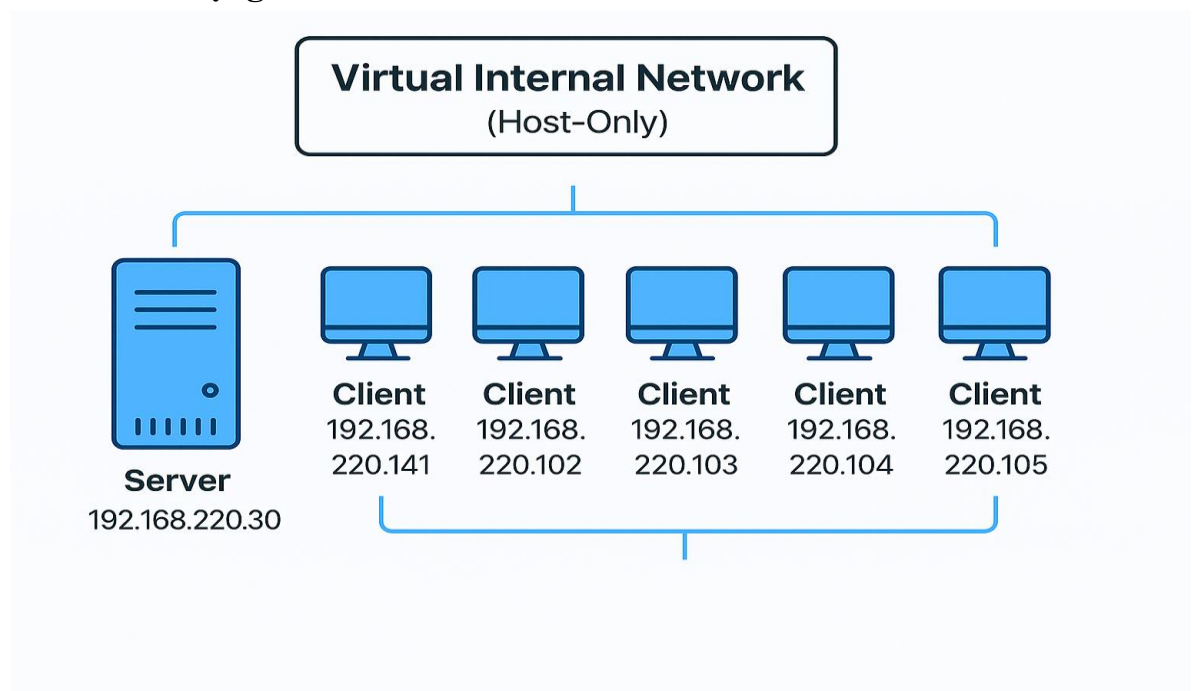
4.1.2. Giới thiệu window sever 2016

Window sever 2016 là hệ điều hành máy chủ do Microsoft phát hành, hỗ trợ triển khai các dịch vụ mạng như DHCP, DNS, File Server và ảo hóa với Hyper-V. Hệ điều hành này có các tính năng nổi bật như Nano Server, Windows Containers và bảo mật nâng cao. Nó được sử dụng rộng rãi trong doanh nghiệp để xây dựng và quản lý hệ thống mạng nội bộ hiệu quả và an toàn.

4.1.3 Giới thiệu window 10

Windows 10 là hệ điều hành dành cho máy tính cá nhân do Microsoft phát hành, ra mắt lần đầu vào tháng 7 năm 2015. Đây là phiên bản cải tiến toàn diện từ Windows 7 và Windows 8, với giao diện hiện đại, dễ sử dụng và hỗ trợ cảm ứng tốt. Windows 10 nổi bật với tính năng đa nhiệm, Cortana (trợ lý ảo), Windows Defender (bảo mật tích hợp), và khả năng tự động cập nhật. Hệ điều hành này được sử dụng phổ biến trên laptop, PC và phù hợp cho cả học tập, làm việc lẫn giải trí.

4.2. Sơ đồ mạng



Hình 4.1. Sơ đồ mạng

4.3. . Mục tiêu thiết kế hệ thống

Mục tiêu của việc thiết kế hệ thống mạng trong đề tài là xây dựng một mô hình mạng đơn giản nhưng đầy đủ chức năng cơ bản, đáp ứng nhu cầu kết nối và quản trị mạng nội bộ trong các môi trường nhỏ như phòng máy, văn phòng, hoặc lớp học thực hành.

Cụ thể, hệ thống được thiết kế nhằm:

- Cung cấp địa chỉ IP tự động cho các máy Client trong mạng thông qua dịch vụ DHCP, giúp giảm công sức cấu hình IP thủ công và hạn chế sai sót.
- Hỗ trợ phân giải tên miền nội bộ nhờ dịch vụ DNS, giúp người dùng truy cập tài nguyên mạng bằng tên dễ nhớ thay vì địa chỉ IP.
- Tối ưu hóa quá trình quản trị mạng, cho phép mở rộng hệ thống dễ dàng mà không cần cấu hình lại toàn bộ địa chỉ IP cho các thiết bị.
- Tăng cường khả năng thực hành và triển khai thực tế cho sinh viên trong môn học Quản trị mạng, thông qua việc áp dụng mô hình mạng đơn giản nhưng mang tính ứng dụng cao.

- Làm nền tảng để phát triển các dịch vụ mạng khác sau này như chia sẻ file, Web Server, Active Directory...

4.4. Mối quan hệ của các dịch vụ

Trong hệ thống mạng được thiết kế, hai dịch vụ chính là **DHCP** và **DNS** đóng vai trò hỗ trợ và bổ trợ lẫn nhau, đảm bảo các máy trạm (Client) có thể kết nối, giao tiếp và truy cập tài nguyên trong mạng một cách hiệu quả. Mối quan hệ giữa các dịch vụ được thể hiện như sau:

- DHCP và DNS phối hợp để tự động cấu hình mạng cho Client
 - Khi một máy Client khởi động và kết nối vào mạng, DHCP Server sẽ tự động cấp:
 - Địa chỉ IP động.
 - Subnet Mask.
 - Gateway (nếu có).
 - Địa chỉ của DNS Server (thường chính là địa chỉ IP của máy Server nội bộ đang giữ vai trò DNS).
 - Nhờ đó, Client không cần cấu hình thủ công bất kỳ thông số nào mà vẫn có thể tham gia vào mạng và phân giải tên miền nội bộ.
- DNS hoạt động nhờ vào cấu hình DHCP
 - DNS Server được cấu hình sẵn các bản ghi tên miền (hostname) trỏ tới IP của các thiết bị trong mạng, điển hình là bản ghi A cho server.ksktp_qtm.trust.
 - DHCP giúp đảm bảo các máy Client biết phải truy vấn DNS ở đâu bằng cách tự động điền đúng địa chỉ DNS.
- Hỗ trợ truy cập tài nguyên bằng tên miền
 - Khi người dùng trên Client cần truy cập tài nguyên từ Server (chẳng hạn thư mục chia sẻ), họ có thể gõ:
\\server.ksktp_qtm.trust
→ DNS sẽ phân giải tên này về IP
→ Client sử dụng IP đó để kết nối đến Server.
- Tính tự động hóa và linh hoạt
 - DHCP giúp thay đổi IP linh hoạt mà không làm gián đoạn truy cập, vì tên miền được quản lý bởi DNS.
 - DNS giúp hệ thống dễ mở **rộng**, chỉ cần thêm bản ghi mới thay vì cấu hình tay IP cho từng Client.

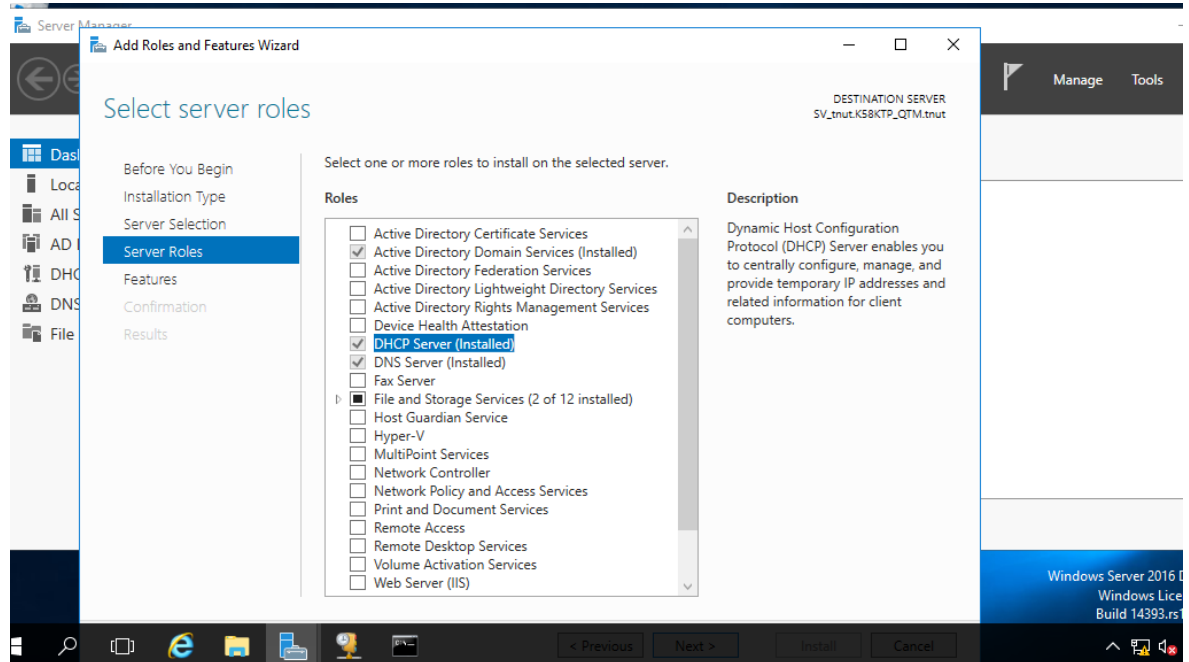
CHƯƠNG 5. Triển Khai Hệ Thống

5.1. Tạo máy ảo

- Tạo 1 sever với ip tĩnh là: 192.168.220.130
- Tạo 5 client với cấu hình mạng Host-only

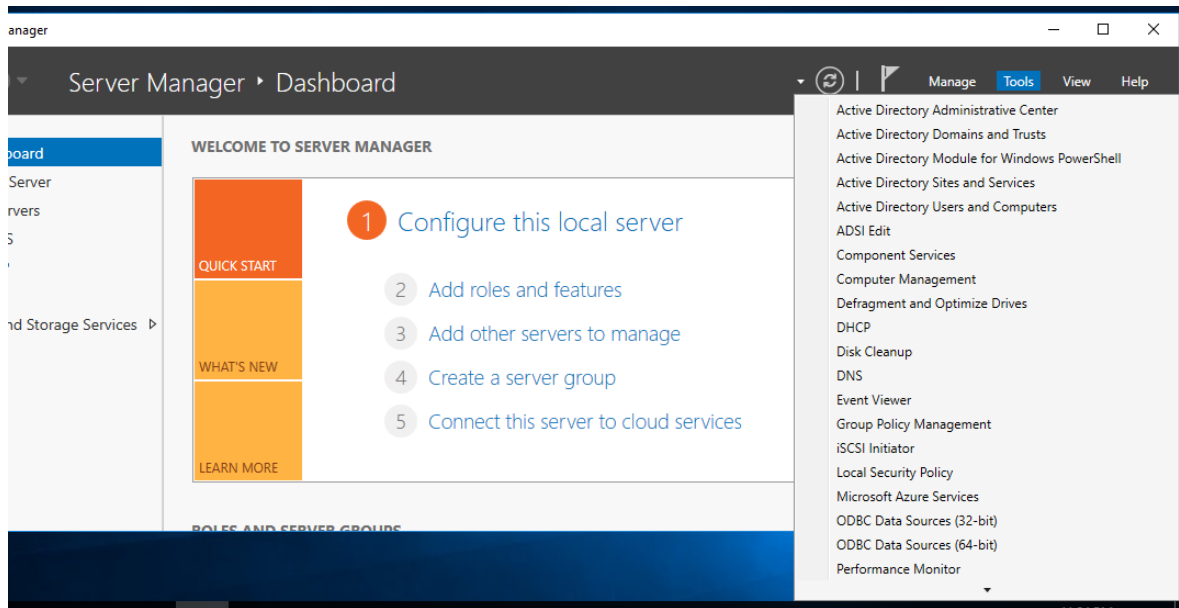
5.2. Cài đặt DHCP sever

Bước 1: Vào sever manager chọn manage → Server roles → tick chọn DHCP sever → next để mở DHCP cho sever



Hình 5.1. Cài đặt DHCP

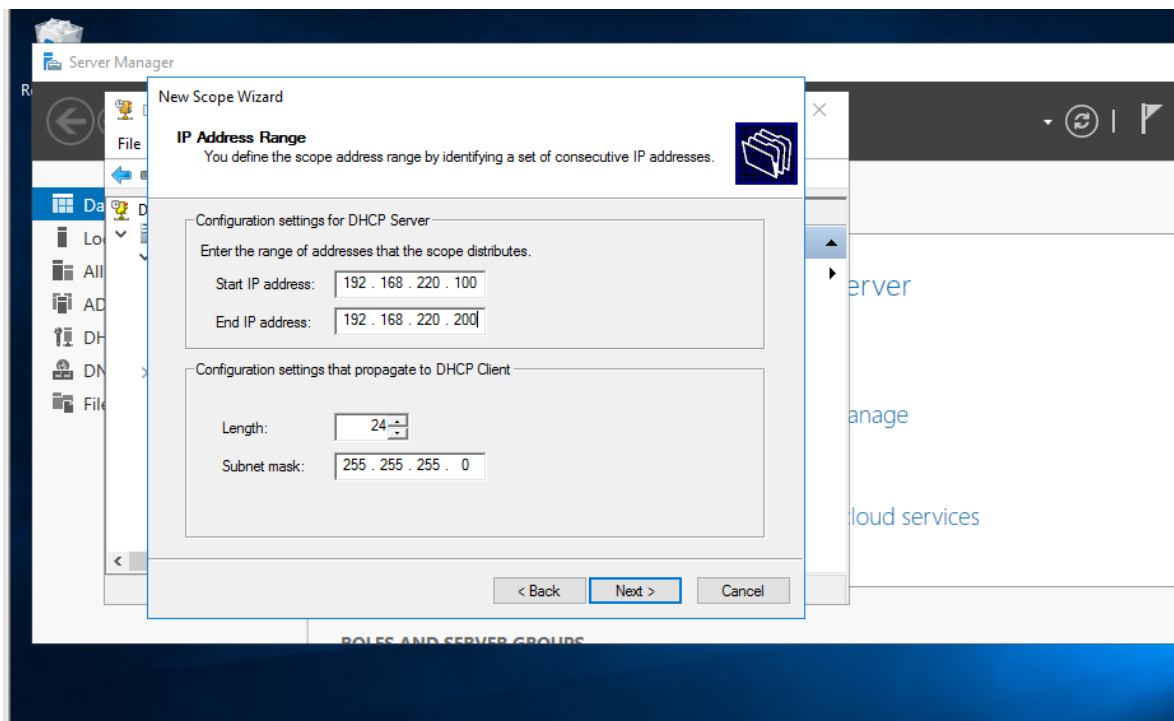
Bước 2: Nhấn vào tool chọn DHCP



Hình 5.2. Chọn cửa sổ DHCP

Bước 3: Trong DHCP chuột phải vào Ipv4 chọn new scope rồi cài đặt
Ở Step: IP Address Range nhập

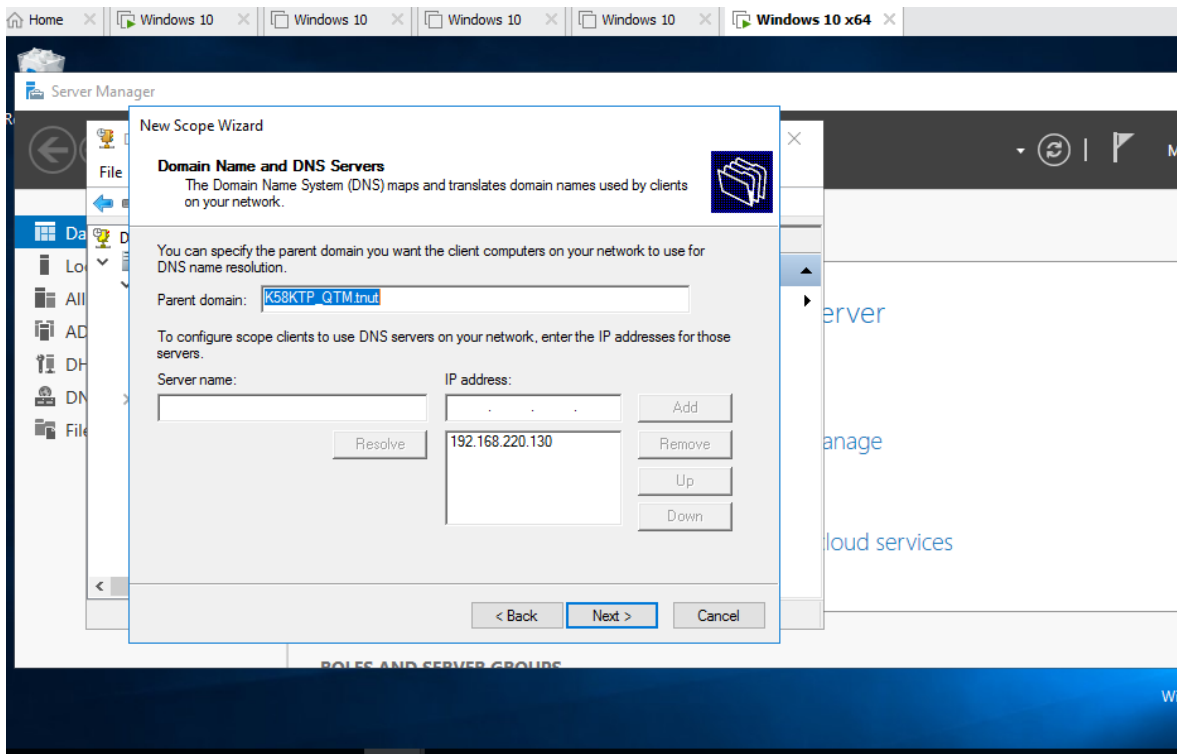
- Start IP: 192.168.220.100
- End IP: 192.168.220.200
- Subnet Mask: 255.255.255.0



Hình 5.3. Setup giải địa chỉ cấp phát

Ở Step: Domain Name and DNS Servers

- Parent domain: K58KTP_QTM.tnut
- DNS Server: 192.168.220.130



Hình 5.4. Cấu hình cho **DHCP Server** cung cấp thông tin **DNS** đến các máy client khi cấp phát IP

Rồi next đến khi cài đặt xong

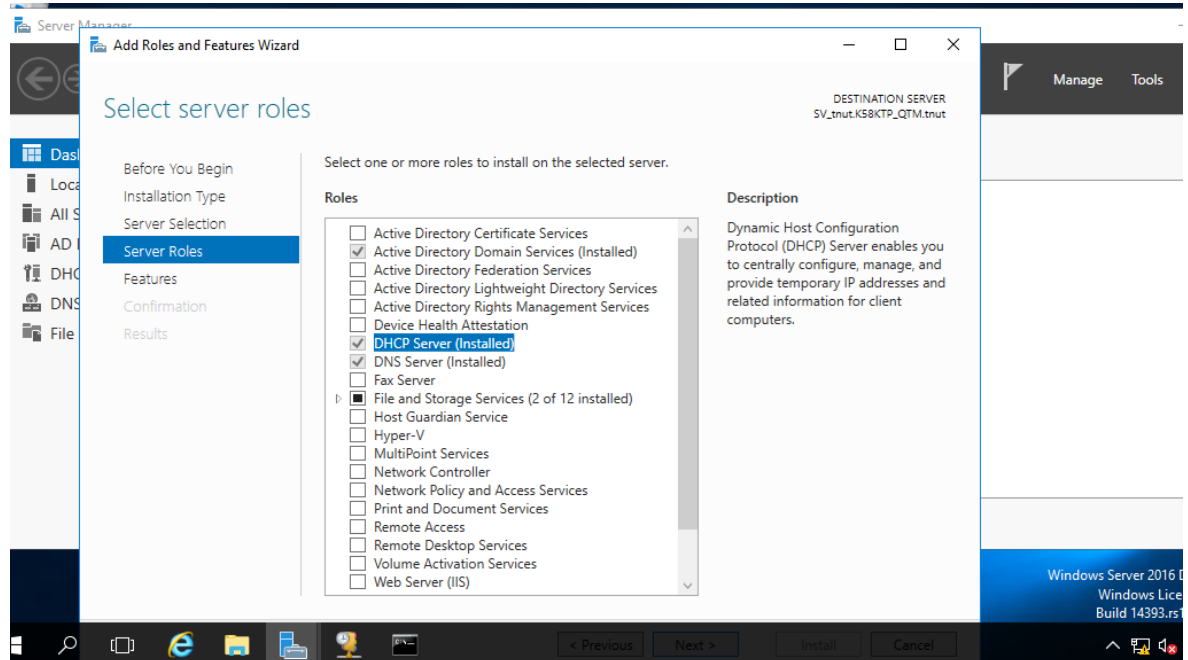
Bước 4: Ra cmd (admin) chạy lệnh để chạy DHCP

```
net stop dhcpserver  
net start dhcpserver
```

Để reset DHCP

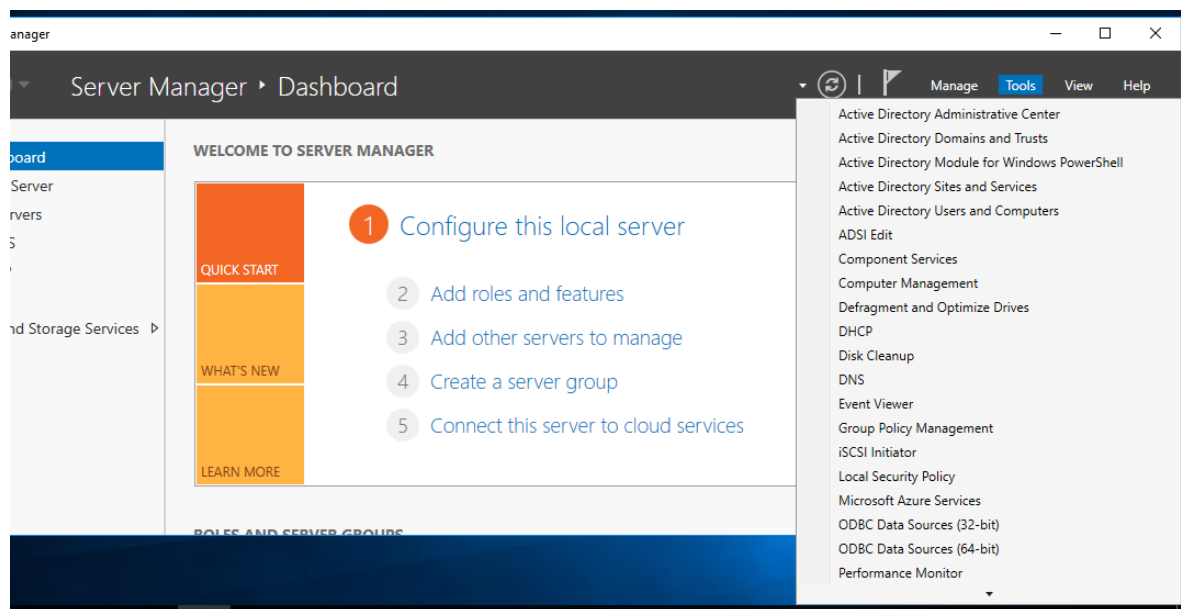
5.3. Cài đặt DNS sever

Bước 1: Vào sever manager chọn manage → sever roles → tick chọn DHCP sever → next để mở DNS cho sever



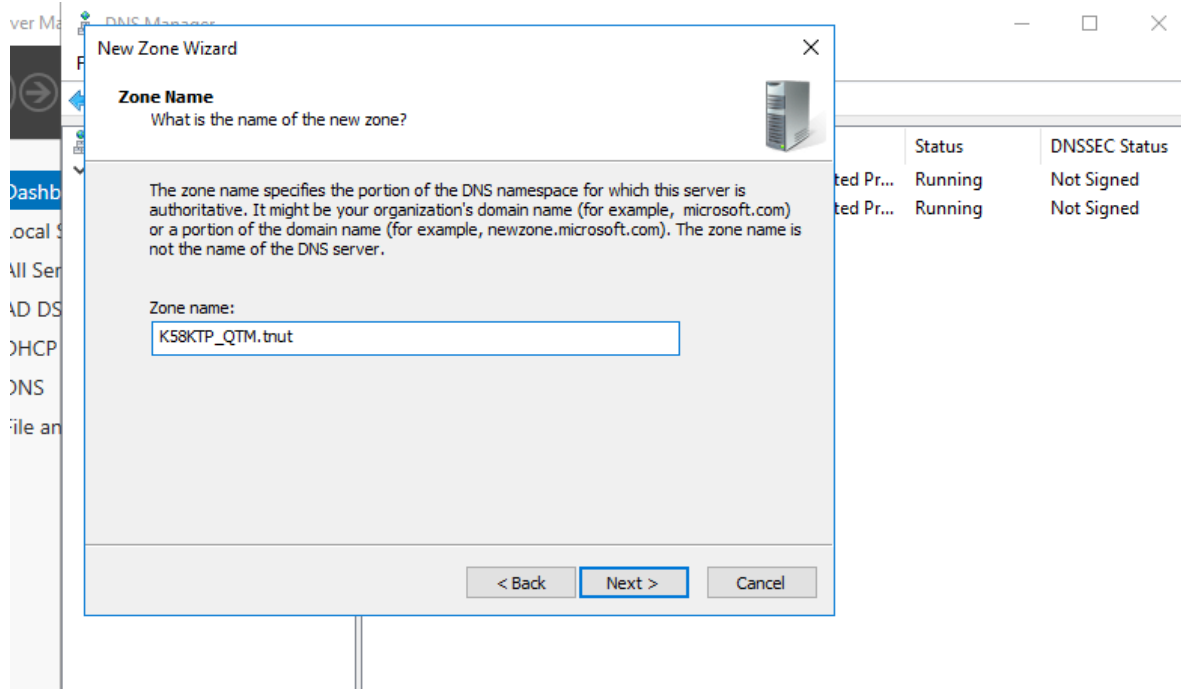
Hình 5.5. Cài đặt DNS

Bước 2: Nhấn vào tool chọn DNS



Hình 5.6. Chọn cửa sổ DNS

Bước 3: Chuột phải vào **Forward Lookup Zones** → New Zone...
Làm theo wizard (lưu ý ở zone name nhập tên domain : K58KTP_QTM.tnut)



Hình 5.7. Tạo mới một DNS zone

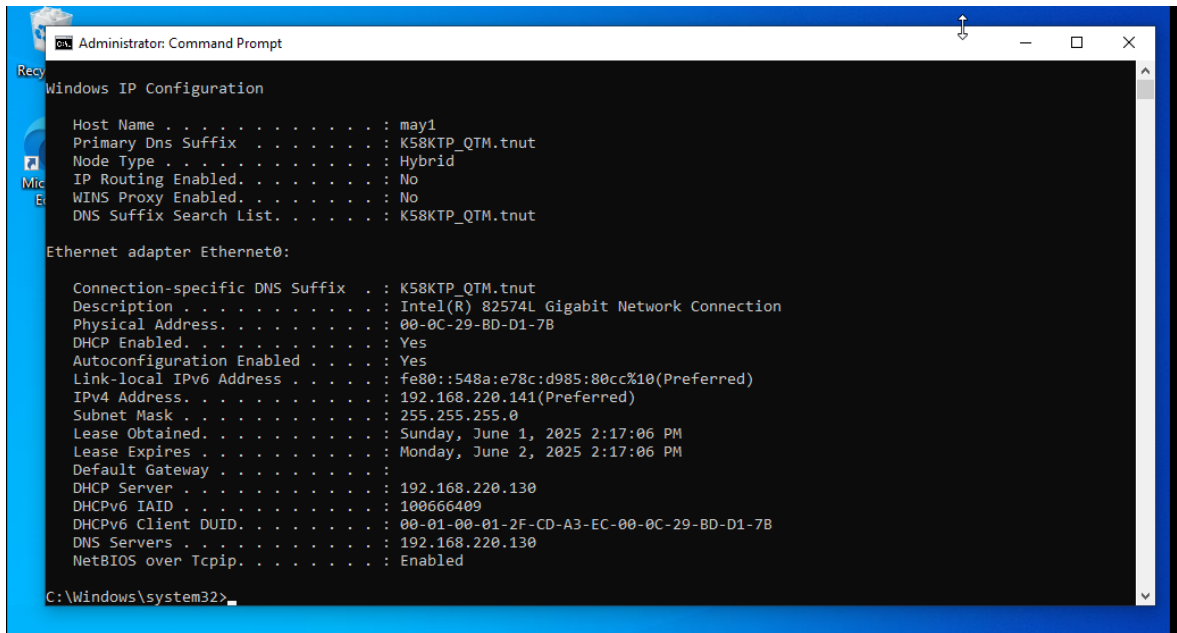
Bước 4: Thêm bản ghi Host (A)

- Click vào zone bạn vừa tạo (K58KTP_QTM.tnut)
- Chuột phải vào vùng trống bên phải → chọn New Host (A or AAAA)...

Tên máy	IP Address
server	192.168.220.130
may1	192.168.220.141
may2	192.168.220.102
may3	192.168.220.103
may4	192.168.220.104
may5	192.168.220.105

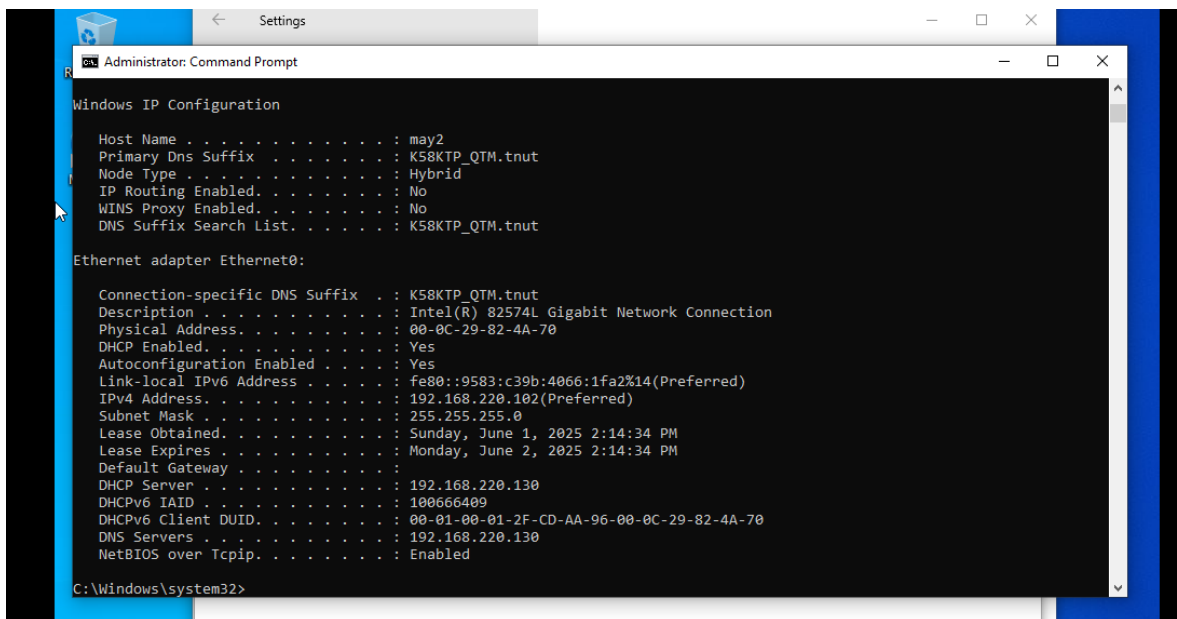
5.4. Kiểm tra hệ thống

Window + R → cmd → nhập ipconfig/all để kiểm tra ip Client 1



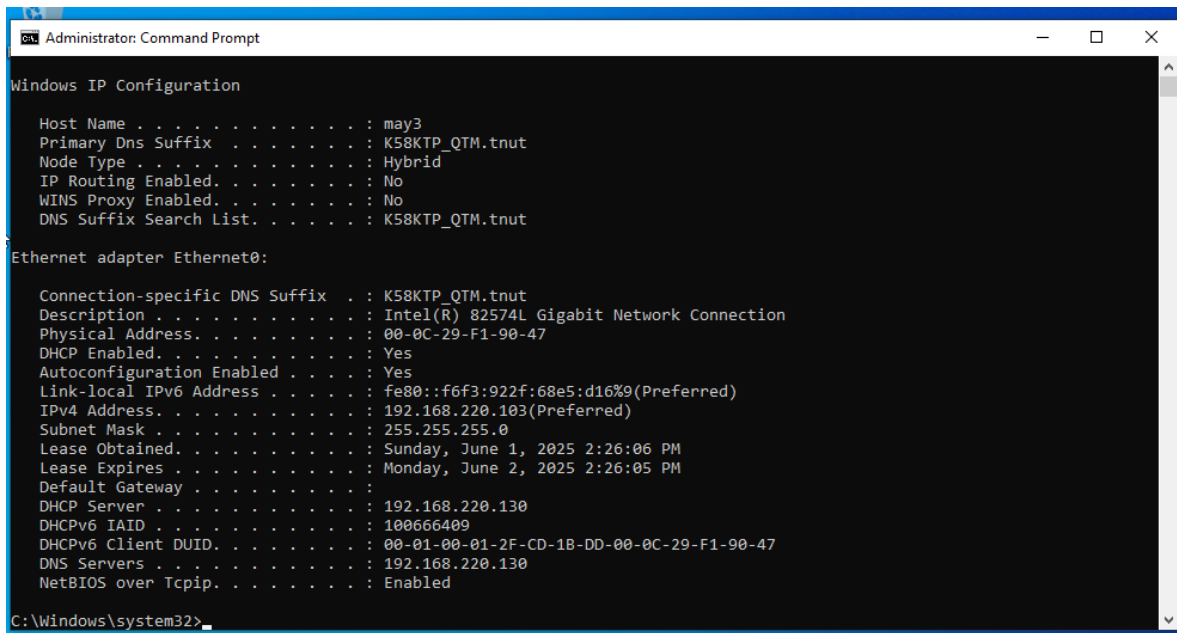
Hình 5.8. Client 1 đã được cấp ip động từ server

Client 2



Hình 5.9. Client 2 đã được cấp ip động từ server

Client 3



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". It displays the output of the "ipconfig /all" command for Client 3. The output is as follows:

```
Windows IP Configuration

Host Name . . . . . : may3
Primary Dns Suffix . . . . . : K58KTP_QTM.tnut
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : K58KTP_QTM.tnut

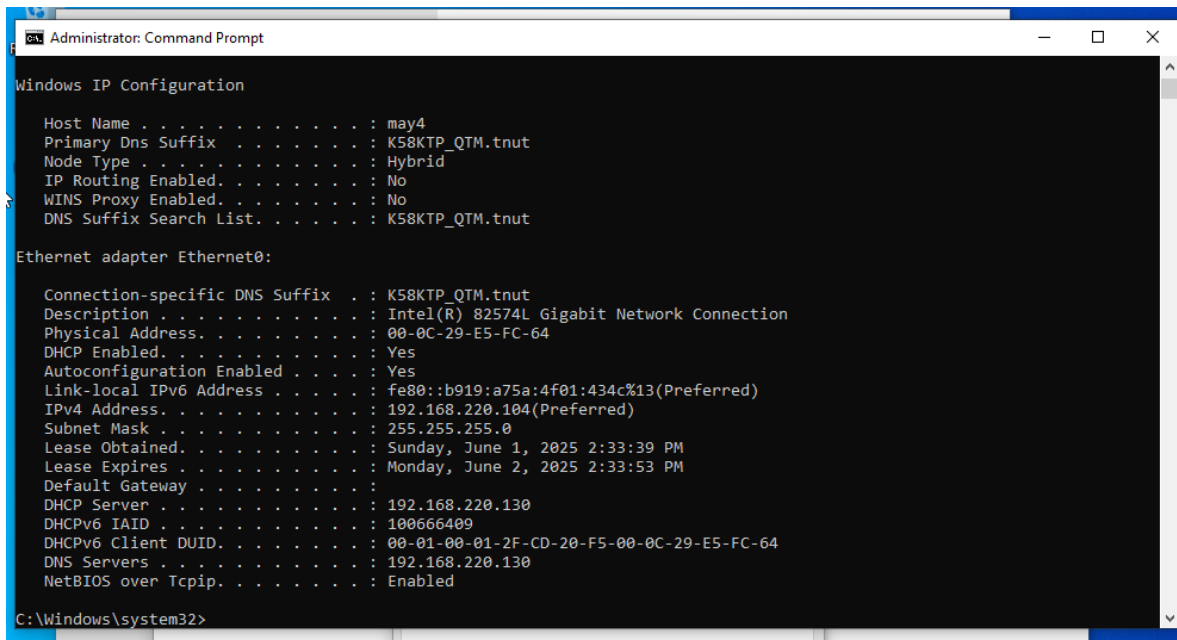
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : K58KTP_QTM.tnut
   Description . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . : 00-0C-29-F1-90-47
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f6f3:922f:68e5:d16%9(Preferred)
   IPv4 Address. . . . . : 192.168.220.103(Preferred)
   Subnet Mask . . . . . : 255.255.255.0
   Lease Obtained. . . . . : Sunday, June 1, 2025 2:26:06 PM
   Lease Expires . . . . . : Monday, June 2, 2025 2:26:05 PM
   Default Gateway . . . . . :
   DHCP Server . . . . . : 192.168.220.130
   DHCPv6 IAID . . . . . : 100666409
   DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-CD-1B-DD-00-0C-29-F1-90-47
   DNS Servers . . . . . : 192.168.220.130
   NetBIOS over Tcpip. . . . . : Enabled

C:\Windows\system32>
```

Hình 5.10. Client 3 đã được cấp ip động từ server

Client 4



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". It displays the output of the "ipconfig /all" command for Client 4. The output is as follows:

```
Windows IP Configuration

Host Name . . . . . : may4
Primary Dns Suffix . . . . . : K58KTP_QTM.tnut
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : K58KTP_QTM.tnut

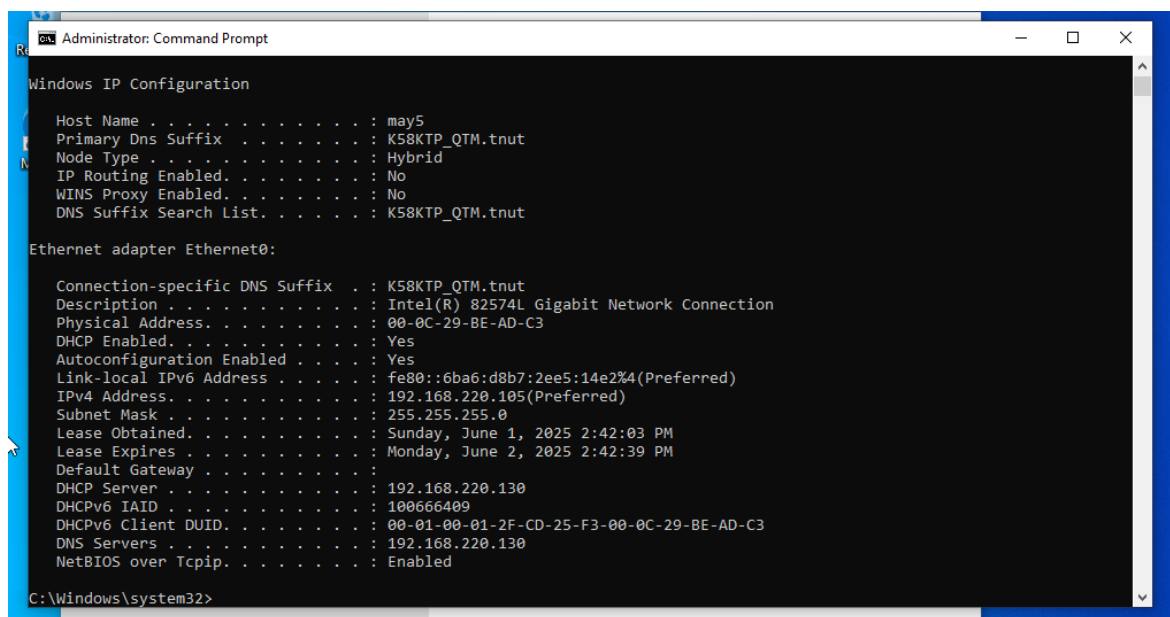
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : K58KTP_QTM.tnut
   Description . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . : 00-0C-29-E5-FC-64
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b919:a75a:4f01:434c%13(Preferred)
   IPv4 Address. . . . . : 192.168.220.104(Preferred)
   Subnet Mask . . . . . : 255.255.255.0
   Lease Obtained. . . . . : Sunday, June 1, 2025 2:33:39 PM
   Lease Expires . . . . . : Monday, June 2, 2025 2:33:53 PM
   Default Gateway . . . . . :
   DHCP Server . . . . . : 192.168.220.130
   DHCPv6 IAID . . . . . : 100666409
   DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-CD-20-F5-00-0C-29-E5-FC-64
   DNS Servers . . . . . : 192.168.220.130
   NetBIOS over Tcpip. . . . . : Enabled

C:\Windows\system32>
```

Hình 5.11. Client 4 đã được cấp ip động từ server

Client 5



```
Administrator: Command Prompt

Windows IP Configuration

Host Name . . . . . : may5
Primary Dns Suffix . . . . . : K58KTP_QTM.tnut
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : K58KTP_QTM.tnut

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : K58KTP_QTM.tnut
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-BE-AD-C3
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::6ba6:d8b7:2ee5:14e2%4(Preferred)
IPv4 Address. . . . . : 192.168.220.105(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, June 1, 2025 2:42:03 PM
Lease Expires . . . . . : Monday, June 2, 2025 2:42:39 PM
Default Gateway . . . . . :
DHCP Server . . . . . : 192.168.220.130
DHCPv6 IAID . . . . . : 100666409
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-CD-25-F3-00-0C-29-BE-AD-C3
DNS Servers . . . . . : 192.168.220.130
NetBIOS over Tcpip. . . . . : Enabled

C:\Windows\system32>
```

Hình 5.12. Client 5 đã được cấp ip động từ server

CHƯƠNG 6. NHẬN XÉT VÀ ĐÁNH GIÁ VỀ HỆ THỐNG

6.1. Những kết quả đã đạt được

- Thiết lập thành công hệ thống mạng nội bộ ảo gồm DHCP và DNS.
- Các máy client nhận IP động từ DHCP server.
- Máy chủ DNS phân giải tên máy nội bộ chính xác.
- Hệ thống hoạt động ổn định trên nền tảng VMware.

Ưu điểm:

- Mô hình đơn giản, dễ mở rộng và quản lý.
- Dễ dàng tích hợp các dịch vụ khác (web, file server) nếu cần.
- Giúp hiểu rõ nguyên lý hoạt động của DHCP và DNS trong môi trường nội bộ

Hạn chế:

- Chưa mô phỏng được truy cập từ Internet.
- Nếu DHCP hoặc DNS server lỗi, toàn hệ thống có thể bị ảnh hưởng.

6.2. Tính thực tiễn của đề tài

- Đề tài triển khai hệ thống mạng gồm 1 server và 5 máy trạm sử dụng dịch vụ DHCP và DNS là một mô hình có tính ứng dụng cao, phù hợp với các hệ thống mạng văn phòng nhỏ, phòng máy tính tại các cơ sở đào tạo, hoặc các doanh nghiệp vừa và nhỏ. Việc cấu hình hai dịch vụ cơ bản – DHCP và DNS là bước đầu tiên để xây dựng một mạng nội bộ có tính tự động hóa, hiệu quả và dễ mở rộng.
- Qua quá trình thực hiện, đề tài cho thấy rõ **lợi ích của DHCP trong việc giảm thiểu thao tác cấu hình thủ công**, giúp quản lý IP hiệu quả hơn, đồng thời **DNS giúp phân giải tên miền, tăng tính tiện dụng và khả năng tổ chức mạng**. Đây là những thành phần không thể thiếu trong bất kỳ hệ thống mạng hiện đại nào.

6.3. Kỹ thuật triển khai

Việc cấu hình các dịch vụ trên nền hệ điều hành Windows Server đòi hỏi người thực hiện phải nắm vững kiến thức về mô hình OSI, giao thức TCP/IP, địa chỉ IP, subnet mask, gateway, v.v.

Trong quá trình triển khai, đề tài đã thực hiện các bước:

- Cài đặt và cấu hình dịch vụ DHCP: tạo DHCP scope, cấp phát IP động, kiểm tra gói tin giao tiếp.

- Cài đặt và cấu hình DNS: tạo bản ghi A, kiểm tra khả năng phân giải tên miền giữa client và server.
- Kiểm tra kết nối giữa các thiết bị, xác minh tính ổn định và chính xác của việc cấp phát địa chỉ IP.

Các bước triển khai được thực hiện thành công, hệ thống hoạt động ổn định, đúng yêu cầu kỹ thuật ban đầu.

6.4. Những ưu điểm và hạn chế của hệ thống

a. Ưu điểm:

- **Tự động hóa cấp phát IP:** Nhờ dịch vụ DHCP, hệ thống không cần cấu hình địa chỉ IP thủ công cho từng máy, tiết kiệm thời gian và giảm thiểu lỗi cấu hình.
- **Phân giải tên miền nhanh chóng:** DNS cho phép các máy client truy cập tài nguyên bằng tên thay vì IP, giúp tăng tính tiện lợi và dễ quản lý.
- **Cấu hình linh hoạt, dễ mở rộng:** Mô hình đơn giản dễ triển khai, có thể mở rộng số lượng client và tích hợp thêm dịch vụ mạng khác khi cần.
- **Tối ưu hóa quản lý mạng nhỏ:** Phù hợp với văn phòng nhỏ, lớp học máy tính, phòng lab – nơi cần một hệ thống gọn, ổn định và dễ giám sát.
- **Rèn luyện kỹ năng thực hành thực tế:** Giúp người thực hiện hiểu sâu hơn về cách hoạt động của DHCP/DNS, kỹ năng xử lý lỗi và làm việc với môi trường server-client.

b. Hạn chế

- **Chưa có tính năng bảo mật nâng cao:** Hệ thống hiện tại chưa tích hợp các cơ chế bảo vệ như DHCP Snooping, DNSSEC hoặc VLAN phân vùng.
- **Khả năng chịu lỗi thấp:** Nếu server gặp sự cố, toàn bộ hệ thống sẽ ngừng cấp IP và phân giải tên, dẫn đến gián đoạn hoạt động mạng.
- **Quản lý hạn chế khi mở rộng lớn:** Khi số lượng client tăng lên đáng kể, mô hình cần bổ sung các công cụ quản lý IP nâng cao như IPAM.
- **Chưa tích hợp giám sát mạng:** Hệ thống chưa có công cụ theo dõi real-time hoặc cảnh báo sự cố mạng.

c. Định hướng phát triển đề tài

Để phát triển và hoàn thiện mô hình hơn trong tương lai, đề tài có thể mở rộng theo các hướng sau:

- **Tích hợp tính năng bảo mật mạng:** Áp dụng DHCP Snooping, cấu hình phân tách VLAN, sử dụng Firewall để kiểm soát truy cập.
- **Thiết lập hệ thống DHCP/DNS dự phòng:** Triển khai mô hình failover hoặc backup server để đảm bảo hệ thống duy trì hoạt động khi có sự cố.
- **Mở rộng sang dịch vụ mạng khác:** Triển khai thêm Web Server, File Server, hoặc Active Directory để mô phỏng môi trường mạng doanh nghiệp hoàn chỉnh.
- **Kết hợp với công cụ giám sát mạng (monitoring):** Sử dụng Wireshark, PRTG hoặc Zabbix để theo dõi lưu lượng, kiểm tra hiệu suất và phát hiện sự cố kịp thời.
- **Triển khai mô hình trên nền tảng ảo hóa hoặc cloud:** Sử dụng VMware, VirtualBox hoặc dịch vụ cloud (Azure, AWS) để học cách triển khai mạng trong môi trường thực tế hiện đại.

KẾT LUẬN

Việc triển khai hệ thống mạng nội bộ ảo sử dụng DHCP và DNS đã giúp chúng em hiểu rõ hơn cách các dịch vụ mạng hoạt động và tương tác với nhau. Đề tài không chỉ mang tính lý thuyết mà còn có khả năng áp dụng thực tiễn trong việc xây dựng hệ thống mạng LAN cho văn phòng nhỏ hoặc hệ thống đào tạo.

TÀI LIỆU THAM KHẢO

- [1] Microsoft Docs. (n.d.). *Install and Configure DHCP on Windows Server*. <https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-deployment>
- [2] Microsoft Docs. (n.d.). *Install DNS Server Role in Windows Server*. <https://learn.microsoft.com/en-us/windows-server/networking/dns/deploy/install-a-dns-server>
- [3] VMware. (n.d.). *Using VMware Workstation to Create Virtual Networks*. docs.vmware.com
- [4] Giới thiệu tóm tắt: DHCP và DNS. <https://www.univention.com/blog-en/2019/03/brief-introduction-dhcp-dns/>