**BÁO CÁO ĐỒ ÁN**

**MÔN AN TÒAN MÁY CHỦ WINDOWS**



**Tìm Hiểu Và Triển Khai Dịch Vụ DHCP, DHCP Fail Over**

Ngành**:** **CÔNG NGHỆ THÔNG TIN**

Chuyên ngành: **CÔNG NGHỆ PHẦN MỀM**

Giảng viên hướng dẫn:

Lớp:

Sinh viên thực hiện:

Thành phố Hồ Chí Minh, năm 2022

**BÁO CÁO ĐỒ ÁN**

**MÔN AN TÒAN MÁY CHỦ WINDOWS**



**Tìm Hiểu Và Triển Khai Dịch Vụ DHCP, DHCP Fail Over**

Ngành**:** **CÔNG NGHỆ THÔNG TIN**

Chuyên ngành: **CÔNG NGHỆ PHẦN MỀM**

Giảng viên hướng dẫn:

Lớp:

Sinh viên thực hiện:

Thành phố Hồ Chí Minh, năm 2022

**MỤC LỤC**

[LỜI CẢM ƠN 4](#_Toc106974689)

[LỜI MỞ ĐẦU 5](#_Toc106974690)

[CHƯƠNG 1. TỔNG QUAN 6](#_Toc106974691)

[**1.1.** **Tổng quan đồ án** 6](#_Toc106974692)

[**1.2.** **Nhiệm vụ đồ án** 6](#_Toc106974693)

[**1.3.** **Cấu trúc đề tài** 6](#_Toc106974694)

[CHƯƠNG 2. CƠ SỞ LÝ THUYẾT 7](#_Toc106974695)

[**2.1.** **Giới thiệu về giao thức DHCP, DHCP FailOver** 7](#_Toc106974696)

[*2.1.1.* *DHCP* 7](#_Toc106974697)

[*2.1.2.* *DHCP FailOver* 7](#_Toc106974698)

[**2.2.** **Lịch sử phát triển của DHCP** 8](#_Toc106974699)

[**2.3.** **Cách thức hoạt động** 8](#_Toc106974700)

[**2.4.** **Cấu trúc thành phần của DHCP** 9](#_Toc106974701)

[**2.5.** **Thông điệp của DHCP** 10](#_Toc106974702)

[**2.6.** **Vai trò của DHCP trong hệ thống mạng** 11](#_Toc106974703)

[**2.7.** **Sự xung đột IP và DHCP** 11](#_Toc106974704)

[**2.8.** **Các tấn công có thể xảy ra với DHCP** 11](#_Toc106974705)

[*2.8.1.* *Máy trạm DHCP Client là bất hợp pháp* 11](#_Toc106974706)

[*2.8.2.* *Máy chủ DHCP Server là bất hợp pháp* 12](#_Toc106974707)

[**2.9.** **Các giải pháp bảo mật của DHCP** 12](#_Toc106974708)

[**2.10.** **Ưu và nhược điểm của DHCP** 13](#_Toc106974709)

[**2.11.** **Đặc tính, đặc điểm của DHCP FailOver** 14](#_Toc106974710)

[CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM 18](#_Toc106974711)

[**3.1.** **Mục tiêu của mô hình ứng dụng** 18](#_Toc106974712)

[**3.2.** **Mô hình ứng dụng** 18](#_Toc106974713)

[**3.3.** **Yêu cầu thực hiện** 18](#_Toc106974714)

[**3.4.** **Các công cụ cần để thực hiện mô hình** 18](#_Toc106974715)

[**3.5.** **Cài đặt DHCP** 19](#_Toc106974716)

[**3.6.** **Tấn công máy chủ DHCP bằng YERSINIA** 32](#_Toc106974717)

[CHƯƠNG 4. KẾT LUẬN VÀ HƯỚNG VÀ PHÁT TRIỂN 39](#_Toc106974718)

[TÀI LIỆU THAM KHẢO 40](#_Toc106974719)

# **LỜI CẢM ƠN**

Trước tiên với tình cảm sâu sắc và chân thành nhất, cho phép chúng em được bày tỏ lòng biết ơn đến tất cả thầy và nhà trường đã tạo điều kiện hỗ trợ, giúp đỡ chúng em trong suốt quá trình học tập và nghiên cứu đề tài này. Trong suốt thời gian từ khi bắt đầu học tập tại trường đến nay, chúng em đã nhận được rất nhiều sự quan tâm, giúp đỡ của Thầy và bạn bè.

Với lòng biết ơn sâu sắc nhất, chúng em xin gửi đến Thầy đã truyền đạt vốn kiến thức quý báu cho chúng em trong suốt thời gian học tập. Nhờ có những lời hướng dẫn, dạy bảo của thầy nên đề tài nghiên cứu của chúng em mới có thể hoàn thiện tốt đẹp.

Một lần nữa, chúng em xin chân thành cảm ơn thầy– người đã trực tiếp giúp đỡ, quan tâm, hướng dẫn chúng em hoàn thành tốt bài báo cáo này trong thời gian qua.

Bài báo cáo thực hiện trong khoảng thời gian không nhiều bước đầu đi vào thực tế của chúng em còn hạn chế và còn nhiều bỡ ngỡ nên không tránh khỏi những thiếu sót. Chúng em rất mong nhận được những ý kiến đóng góp quý báu của Thầy để kiến thức của chúng em trong lĩnh vực này được hoàn thiện hơn đồng thời có điều kiện bổ sung, nâng cao kiến thức của mình.

Chúng em xin chân thành cảm ơn!

|  |
| --- |
| SSinh viên thực hiện |

# **LỜI MỞ ĐẦU**

Hiện nay ngành công nghệ kỹ thuật điện tử phát triển nhanh với công nghệ ngày càng tiên tiến và hiện đại. Một trong những thành tựu lớn nhất mà ngành điện tử mang lại cho cuộc sống con người là mạng máy tính. Đây là một môi trường thông tin liên kết con người trên toàn cầu lại với nhau, việc trao đổi thông tin bây giờ đã trở nên nhanh chóng, tiện lợi hơn bao giờ hết. Mạng máy tính được hình thành từ nhu cầu muốn chia sẻ tài nguyên và dùng chung nguồn dữ liệu. Máy tính cá nhân là công cụ tuyệt vời giúp tạo dữ liệu, bảng tính, hình ảnh và nhiều dạng thông tin khác nhưng không cho phép chia sẻ dữ liệu ta đã tạo nên. Nếu không có hệ thống mạng, dữ liệu phải được in ra giấy thì người khác mới có thể hiệu chỉnh và sử dụng được hoặc chỉ có thể sao chép lên đĩa mềm do đó tốn nhiều thời gian và công sức.

Trong môi trường Windows, các phần mềm ứng dụng và các dịch vụ mạng ra đời nhằm giải quyết các vấn đề chuyên môn một cách hữu hiệu. Bên cạnh đó việc quản trị chúng là một công việc không hề đơn giản,đòi hỏi mọi người phải quan tâm.

Thấy được tầm quan trọng của mạng máy tính nên em chọn đề tài:“Tìm hiểu và triển khai dịch vụ DHCP, DHCP Fail Over”. Đề tài này sẽ hướng dẫn từng bước để có thể xây dựng 1 mô hình mạng. Hy vọng nó sẽ là 1tài liệu hữu ích, không chỉ cho những người mới làm quen với mang và hệ thống, mà còn giúp cho chúng ta đang tìm hiểu về vấn đề này tích lũy thêm kiến thức.

# **CHƯƠNG 1. TỔNG QUAN**

## **Tổng quan đồ án**

Đồ án sẽ giới thiệu cho chúng ta biết về giao thức DHCP, DHCP Fail Over và nhiệm vụ của giao thức.

## **Nhiệm vụ đồ án**

Giúp người dùng sử dụng trong những mục đích sau:

* Cấu hình địa chỉ IP đáng tin cậy
* Giảm quản trị mạng

## **Cấu trúc đề tài**

Đồ án gồm có 4 chương:

**Chương 1. Tổng Quan**

Phần này giới thiệu tổng quan về đồ án, nhiệm vụ đồ án, giúp chúng ta hiểu được nội dung cơ bản của nó.

**Chương 2. Cơ sở lý thuyết**

Phần này giới thiệu cụ thể về: Giới thiệu DHCP, DHCP FailOver; Lịch sử phát triển của DHCP; Cách thức hoạt động của DHCP, DHCP FailOver; Ưu và nhược điểm của DHCP; Cấu trúc thành phần của DHCP; Thông điệp của DHCP; Vai trò của DHCP trong hệ thống mạng; Sự xung đột IP và DHCP; Các tấn công có thể xảy ra với DHCP; Các giải pháp bảo mật DHCP; Đặc tính của DHCP Fail Over.

**Chương 3. Kết quả thực nghiệm**

Phần này sẽ cho chúng ta thấy mô hình mục tiêu ứng dụng, giới thiệu các công cụ để thực hiện và phân tích các gói tin trong wireshark.

**Chương 4. Kết luận và hướng phát triển**

Phần này sẽ rút ra những lưu ý và lời khuyên khi sử dụng giao thức DHCP, DHCP Failover và đưa ra hướng phát triển để giao thức hoàn thiện hơn.

# **CHƯƠNG 2. CƠ SỞ LÝ THUYẾT**

## **Giới thiệu về giao thức DHCP, DHCP FailOver**

### *DHCP*

* **DHCP**

DHCP (Dynamic Host Configuration Protocol) là giao thức cấp phát địa chỉ IP tự động được thiết kế nhằm giảm tính phức tạp cho việc cấu hình địa chỉ IP quản trị.

DHCP có nhiệm vụ giúp quản lý nhanh, tự động và tập trung phân phối địa chỉ IP bên trong một mạng, cho phép chúng ta truy cập internet.

Trường hợp các máy tính không có DHCP thì có thể cấu hình IP thủ công (hay còn gọi là cấu hình IP tĩnh). Hiện nay, DHCP có 2 version sử dụng cho IPv4 và IPv6.

Ngoài ra, nó cũng đảm bảo không có trường hợp hai hay nhiều thiết bị có cùng địa chỉ IP, đồng thời, cung cấp một số thông tin cần thiết cho hoạt động của mạng như dịch vụ DNS, subnet mask (mặt nạ mạng) hay default gateway (cổng mặc định) mang thông tin đến các thiết bị chính xác, hợp lý hơn.

* **DHCP Server**

DHCP server là một máy chủ thực hiện việc kết nối mạng. Nó có chức năng phản hồi thông tin khi máy trạm (DHCP client) phát yêu cầu. Ngoài ra, DHCP server còn có nhiệm vụ truyền thông tin một cách hợp lý nhất đến các thiết bị, đồng thời, thực hiện cấu hình cổng mặc định (Default gateway) hay Subnet mask.

### *DHCP FailOver*

DHCP FailOver là một cơ chế cho phép 2 DHCP Server cùng chia sẻ chung dịch vụ DHCP, tăng độ sẵn sàng và phục vụ liên tục trong hệ thống mạng.

Hai máy chủ DHCP sẽ chuyển đổi và sao chép thông tin địa chỉ IP và cấu hình tùy chọn trong một subnet hoặc scope, đảm bảo khả năng cung cấp dịch vụ DHCP liên tục cho các máy khách.

Khi một máy chủ DHCP không khả dụng, máy chủ khác sẽ chịu trách nhiệm cấp phát địa chỉ IP cho các máy khách.

DHCP failover cung cấp hỗ trợ tối đa hai máy chủ DHCP và có mối quan hệ chuyển đổi dự phòng (failover relationship) được giới hạn trong phạm vi và mạng con IPv4.

## **Lịch sử phát triển của DHCP**

DHCP đầu tiên được định nghĩa trong RFC 1531 vào tháng 10/1993, là phần mở rộng của Bootstrap Protocol (BOOTP). Động cơ để cải tiến BOOTP là BOOTP đòi hỏi phải cấu hình thủ công để thêm thông tin cho từng máy client, và không cung cấp cơ chế tái sử dụng lại địa chỉ IP.

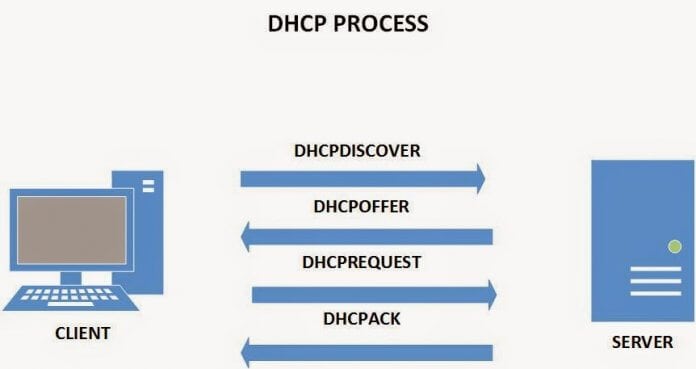
Năm 1997, [*RFC 2131*](http://tools.ietf.org/html/2131) ra đời, vẫn còn chuẩn IPv4 cho đến năm 2011. DHCPv6 được định nghĩa trong [*RFC 3315*](http://tools.ietf.org/html/3315)*,*[*RFC 3633*](http://tools.ietf.org/html/3633) được thêm vào DHCPv6 cơ chế prefix delegation.

Giao thức BOOTP lần đầu tiên được định nghĩa trong [*RFC 951*](http://tools.ietf.org/html/951) thay thế cho RARP (Reverse Address Resolution Protocol), mà động cơ thiết yếu để thay thế RARP bằng BOOTP là RARP hoạt động ở tầng data link, điều này làm cho việc thực hiện trên nhiều máy server trở nên khó khăn, và đòi hỏi một server xử lý trên riêng trên từng network. BOOTP có đổi mới relay agent, cho phép forwarding đến gói BOOTP trong mạng cục bộ, vì vậy BOOTP server có thể phục vụ cho nhiều IP subnet.

## **Cách thức hoạt động**

Cách thức hoạt động của DHCP có thể hiểu một cách ngắn gọn là khi một thiết bị yêu cầu địa chỉ IP từ một router thì ngay sau đó router sẽ gán một địa chỉ IP khả dụng cho phép thiết bị đó có thể giao tiếp trên mạng.

Như ở các hộ gia đình hay các doanh nghiệp nhỏ thì router sẽ hoạt động như một máy chủ DHCP nhưng ở các mạng lớn hơn thì DHCP như một máy chỉ ở vai trò là máy tính.

*Hình 2.3.1. Các giai đoạn của DHCP*

Cách thức hoạt động của DHCP còn được giải thích ở một cách khác thì khi một thiết bị muốn kết nối với mạng thì nó sẽ gửi một yêu cầu tới máy chủ, yêu cầu này gọi là **DHCP DISCOVER.**

Sau khi yêu cầu này đến máy chủ DHCP thì ngay tại đó máy chủ sẽ tìm một địa chỉ IP có thể sử dụng trên thiết bị đó rồi cung cấp cho thiết bị địa chỉ cùng với gói **DHCP OFFER**

Khi nhận được IP thì thiết bị tiếp tục phản hồi lại máy chủ DHCP gói mang tên **DHCP REQUEST.**

Lúc này là lúc chấp nhận yêu cầu thì máy chủ sẽ gửi tin báo nhận **(ACK)** để xác định thiết bị đó đã có IP, đồng thời xác định rõ thời gian sử dụng IP vừa cấp đến khi có địa chỉ IP mới.

## **Cấu trúc thành phần của DHCP**

Khi làm việc với DHCP, cần phải hiểu tất cả thành phần của nó. Dưới đây là danh sách các thành phần của DHCP.

* **DHCP Sever:** Là thiết bị đóng vai trò là máy chủ có nhiệm vụ nhận yêu cầu và cấp phát địa chỉ IP đến các DHCP Client.
* **DHCP Cilent:** Là các thiết bị có thể kết nối với mạng Internet như điện thoại, laptop, máy tính, máy in, tivi,… và chúng sẽ giao tiếp với máy chủ DHCP để nhận IP truy cập mạng.
* **DHCP Lease:** Là thời gian mà thiết bị sử dụng 1 địa chỉ IP trước khi gia hạn. Mỗi IP khi được cấp phát đều có thời gian sử dụng nhất định và được cấp địa chỉ mới khi hết hạn.
* **DHCP Relay agents:** Đóng vai trò là thiết bị trung gian giúp kết nối DHCP Client và DHCP Server. Thiết bị này thường chỉ xuất hiện trong các mô hình mạng lớn và có nhiều kết nối phức tạp.
* **Binding:** Là một tập hợp chứa các thông tin cầu hình trong đó có chưa ít nhất 1 địa chỉ IP đã được cấp phát đến 1 DHCP Client và máy chủ DHCP sẽ quản lý các kết nối này.

## **Thông điệp của DHCP**

* **DHCP Discover:** là một gói tin được gửi đến DHCP Server từ một thiết bị Client khi muốn truy cập mạng để yêu cầu thông tin địa chỉ IP.
* **DHCP Offer:** Sau khi nhân được DHCP Discover thì DHCP Server sẽ gửi gói tin chứa thông tin địa chỉ IP và cấu hình TCP/IP bổ sung cho máy tính Client.
* **DHCP Request:** Là gói thông tin do DHCP client lại cho máy chủ DHCP sau khi tiếp nhận DHCP Offer nhằm xác nhận đã chấp nhận địa chỉ IP được cấp phát.
* **DHCP Release:** Do DHCP Client gửi đến server để thông báo giải phóng địa chỉ IP cùng lúc đó Client sẽ tiến hành xóa thuê bao đang tồn tại.
* **DHCP Acknowledge:** Khi xác nhận DHCP Request của máy Client thì DHCP gửi lại gói DHCP acknowledge và kèm theo đính hướng tham số để Client có thể tham gia mạng TCP/IP.
* **DHCP Nak:** Đối với các địa chỉ IP không còn giá trị sử dụng hoặc được sử dụng bởi 1 máy khác thì DHCP server thực hiện gửi gói DHCP Nak để thông báo cho Client thuê bao lại IP.
* **DHCP Decline:** Được gửi đến các DHCP server khi Client thực hiện quyết định tham số thông tin không còn giá trị và tiến hành thuê bao lại.

## **Vai trò của DHCP trong hệ thống mạng**

* Giúp công tác quản trị hệ thống mạng được tự động, tiện lợi và tập trung.
* Bằng cách tự động gán địa chỉ IP cho thiết bị khi truy cập internet, tiết kiệm rất nhiều thời gian so với cấu hình thủ công, giảm rủi ro phát sinh lỗi.
* **Tại sao sử dụng dịch vụ DHCP?**
* DHCP đóng vai trò tự động cấp IP và cung cấp các thông số truy cập mạng. Từ đó, giúp công tác quản trị trở nên đơn giản hơn rất nhiều.
* Giảm tối đa khả năng phát sinh lỗi do cấu hình thủ công.

## **Sự xung đột IP và DHCP**

* DHCP có thể giảm rủi ro gặp lỗi trùng IP bằng cách tự động gán địa chỉ IP cho các thiết bị. Tuy nhiên, trong trường hợp bản thân DHCP gặp lỗi cũng là nguyên nhân dẫn đến lỗi xung đột IP.
* **Cách xử lý**: Trong trường hợp này, người quản trị chỉ cần giải phòng IP bị trùng. Nếu vấn đề không được giải quyết chỉ cần khởi động lại router. Khi đã dùng cả hai cách nhưng vẫn không giải quyết được, có thể vấn đề không nằm ở phạm vi router hoặc **DHCP.**

## **Các tấn công có thể xảy ra với DHCP**

### *Máy trạm DHCP Client là bất hợp pháp*

* Đây là trường hợp tấn công DHCP từ máy Client khi bị mất quyền kiểm soát sẽ liên tục thực hiện gửi yêu cầu IP về DHCP Server.
* Khi nhận được yêu cầu, Server sẽ tự động cấp phát IP liên tục cho các client không xác thực.
* Đến khi hết địa chỉ IP dẫn đến cạn kiệt IP cần thiết cho các máy Client hợp pháp, lúc này hiện tượng không truy cập được mạng hoặc tốc độ truy cập yếu sẽ xuất hiện trên các thiết bị.
* Đây là kiểu tấn công đơn giản, dễ thực hiện, chỉ cần băng thông và không tốn nhiều thời gian.

### *Máy chủ DHCP Server là bất hợp pháp*

Ngược lại đối với tình huống DHCP bị tấn công khi máy chủ DHCP Server là bất hợp pháp do kẻ tấn công trực tiếp phá vỡ hàng rào bảo vệ mạng.

Lúc này kẻ tấn công kiểm soát được DHCP và điều khiển tất cả các thao tác trên hệ thống mạng.

Dưới đây là 3 kiểu tấn công khi máy chủ **DHCP server** là bất hợp pháp thường gặp:

* DoS hệ thống mạng: Kẻ tấn công sẽ thiết lập một dải IP và subnet mask làm cho máy trạm không thể truy cập vào hệ thống mạng và dẫn đến tình trạng DoS trong hệ thống.
* DNS redirect: Là cách tấn công gián tiếp thông qua thao tác đổi DNS dẫn máy trạm truy cập vào các trang web chứa mã độc hoặc các trang web giả mạo có. Từ đó chúng đánh cắp thông tin của người dùng máy chủ Client.
* Man-in-the-middle: Là kiểu tấn công mà cổng mặc định sẽ được biến đổi về máy của kẻ tấn công. Từ đó, sao chép và đánh cắp toàn bộ thông tin người dùng, toàn bộ thông tin, yêu cầu từ Client gửi đến Gateway mặc định sẽ chuyển đến máy của chúng trước khi trở về.

## **Các giải pháp bảo mật của DHCP**

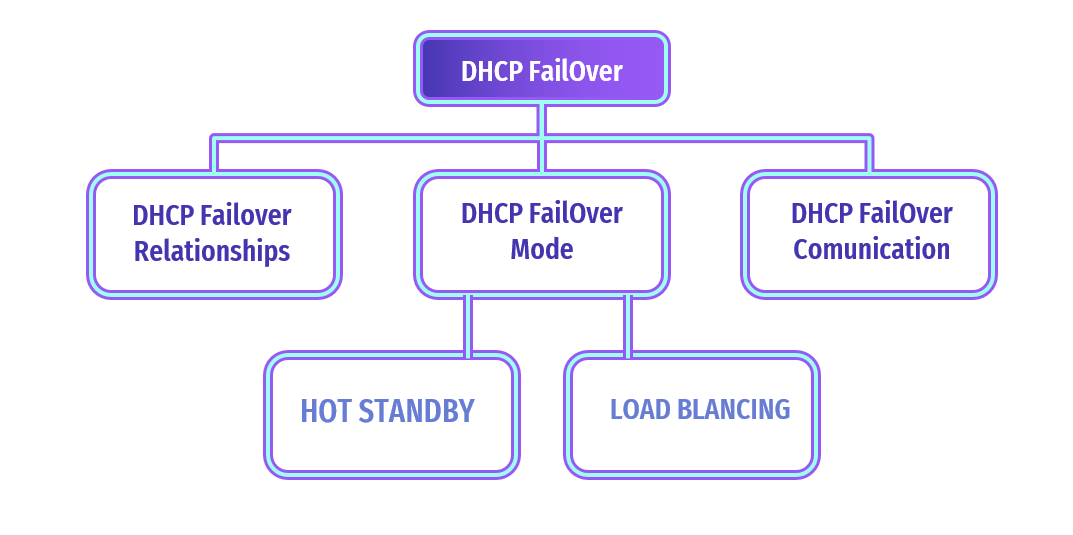
* **Với tấn công bằng cách sử dụng DHCP Client bất hợp pháp**
* Đối với kiểu tấn công này, có thể dùng những switch có khả năng bảo mật cao giúp hạn chế số lượng địa chỉ MAC được dùng trên một cổng.
* Cách này hạn chế việc trong cùng một khoảng thời gian. Cùng một cổng có quá nhiều địa chỉ MAC được sử dụng.
* Trường hợp số lượng địa chỉ vượt quá mức quy định, cổng sẽ bị đóng lại, ngừng phục vụ và chỉ hoạt động trở lại theo thời gian mà quản trị viên đã thiết lập.
* **Với kiểu tấn công Man-in-the-middle**
* Khi gặp kiểu tấn công Man-in-the-middle, ta có thể dùng các switch có tính năng bảo mật DHCP snooping cao.
* Bằng cách này sẽ hạn chế kết nối DHCP đến các cổng không đáng tin, chỉ các cổng được tin tưởng mới được cho phép gói tin DHCP response hoạt động và chỉ cổng này được quản trị viên cho kết nối đến server thật.
* **Một số giải pháp bảo mật DHCP Server thường dùng**
* Sử dụng hệ thống tập tin NTFS để lưu trữ dữ liệu an toàn và bảo mật hơn.
* Cập nhật thường xuyên các phiên bản mới cho phần mềm và windows.
* Quét virus thường xuyên cho hệ thống.
* Loại bỏ các phần mềm hoặc dịch vụ không cần thiết.
* Không nên tải hoặc sử dụng những phần mềm không có độ uy tín cao hoặc có dấu hiệu lừa đảo, giả mạo.
* Sử dụng tường lửa cho máy chủ DHCP trong hệ thống mạng.
* Bảo mật vật lý cho máy chủ bằng mật khẩu 2 lớp, xác thực danh tính,…

## **Ưu và nhược điểm của DHCP**

* **Ưu điểm**
* Giúp các thiết bị kết nối mạng nhanh chóng từ máy tính, laptop, điện thoại,…
* Khi nhiều thiết bị có yêu cầu truy cập mạng đều nhận được địa chỉ IP gần như ngay lập tức nhờ những cài đặt mặc định cũng như thuật toán lấy địa chỉ tự động của DHCP => Nhờ đó DHCP quản lý mạng mạng hơn và ổn định hơn.
* Các nhà quản trị mạng có thể thay đổi cấu hình và thông số của IP để nâng cấp cơ sở hạ tầng.
* Các thiết bị có thể di chuyển tự do từ mạng này sang mạng khác và nhận IP mới tự động.
* Giúp người quản lý có thể theo dõi các thông số liên quan đến địa chỉ IP một cách trực quan và tiện lợi hơn khi quản lí IP và các tham số dễ dàng qua các trạm.
* Quản lý địa chỉ IP một cách khoa học, tránh trường hợp trùng IP trên nhiều, đảm bảo cấu hình tự động cho mọi thiết bị kết nối mạng giúp vận hành hệ thống linh hoạt và ổn địng hơn.
* **Nhược điểm**
* Việc sử dụng IP động của DHCP không phù hợp với các thiết bị cố định và cần truy cập liên tục như máy in, file server.
* DHCP thường chỉ được sử dụng tại các hộ gia đình hoặc mô hình mạng nhỏ.

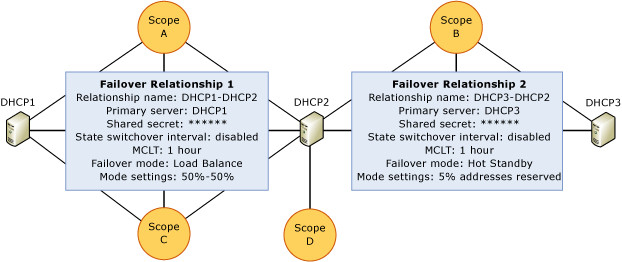
## **Đặc tính, đặc điểm của DHCP FailOver**

DHCP Failover hỗ trợ DHCP Server duy trì liên lạc với nhau thông qua TCP/IP và có thể cấu hình trực tiếp DHCP Failover mà không cần ngừng lại hoặc khởi động lại dịch vụ DHCP.

* 1 Scope chỉ cho hỗ trợ tối đa 2 DHCP Server chạy Failover với nhau.
* 1 trong 2 máy DHCP Server có thể tự động thiết lập việc nhân rộng và đồng bộ hóa cho nhau.
* Client phải giao tiếp được cả 2 DHCP Server, có thể là trực tiếp hoặc có thể nhờ DHCP Relay.

*Hình 2.11.1. Đặc điểm của DHCP FailOver*

* **DHCP FailOver Realationships**
* DHCP 1 và DHCP 2 có thể thiết lập failover là nhờ vào Failover Relationships. Nó giống như là một kênh để 2 DHCP Server giao tiếp với nhau.

*Hình 2.11.1. Giao tiếp giữa 2 DHCP*

* Thuộc tính của Failover Relationship gồm:
* Một mối quan hệ (Failover Relationship) chỉ hỗ trợ tối đa 2 DHCP Server.
* Một máy chủ DHCP không thể có nhiều hơn 31 mối quan hệ chuyển đổi dự phòng.
* Xóa mối quan hệ chuyển đổi dự phòng sẽ xóa chuyển đổi dự phòng khỏi tất cả các phạm vi liên quan đến mối quan hệ đó.
* Không cần thiết phải tạm dừng, dừng hoặc khởi động lại dịch vụ Máy chủ DHCP khi thêm, xóa hoặc sửa đổi các mối quan hệ chuyển đổi dự phòng.
* Mối quan hệ chuyển đổi dự phòng không hỗ trợ phạm vi IPv6.
* Một phạm vi DHCP chỉ có thể được liên kết với một mối quan hệ chuyển đổi dự phòng tại một thời điểm. Tuy nhiên, các phạm vi có thể bị xóa khỏi một mối quan hệ chuyển đổi dự phòng và thêm vào một mối quan hệ chuyển đổi dự phòng khác.
* **DHCP FailOver Mode**
* **Hot Standby (Active –Passive)**
* Sẽ có một server là *active* và server còn lại là *standby*. Server chạy active sẽ chịu trách nhiệm phục vụ cấp địa chỉ IP trong mạng khi client yêu cầu. Server chạy standby còn lại là để dự phòng và không phục vụ, chỉ khi DHCP Server Active chết thì nó mới đứng ra thay thế.
* Ở chế độ này, hai máy chủ hoạt động trong mối quan hệ chuyển đổi dự phòng trong đó một máy chủ đang hoạt động chịu trách nhiệm cho thuê địa chỉ IP và thông tin cấu hình cho tất cả các máy khách trong một phạm vi hoặc mạng con.
* Máy chủ đối tác đảm nhận vai trò dự phòng, với trách nhiệm chỉ cấp giấy thuê cho máy khách DHCP nếu máy chủ đang hoạt động không khả dụng.
* Chế độ này là lý tưởng cho các tình huống mà đối tác chuyển đổi dự phòng chỉ được sử dụng tạm thời khi máy chủ hoạt động không khả dụng.



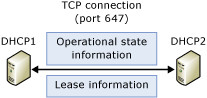
*Hình 2.11.2. Host Standby*

* **Load Blancing**
* Chế độ cân bằng tải là chế độ triển khai mặc định. Trong chế độ này, hai máy chủ DHCP đồng thời phục vụ địa chỉ IP và các tùy chọn cho các máy khách trên một mạng con nhất định. Các yêu cầu máy khách DHCP được cân bằng tải và được chia sẻ giữa hai máy chủ DHCP. Tỷ lệ cân bằng tải mặc định giữa hai máy chủ là 50:50, nhưng tỷ lệ này có thể được tùy chỉnh theo bất kỳ tỷ lệ nào từ 0 đến 100%.



*Hình 2.11.3. Load Blancing*

* **DHCP FailOver Comunication**
* Cả hai máy chủ DHCP trong mối quan hệ chuyển đổi dự phòng phải duy trì kết nối TCP liên tục với nhau.
* Các đối tác chuyển đổi dự phòng DHCP thiết lập và duy trì kết nối này trên cổng 647 và sử dụng nó để trao đổi thông tin trạng thái hoạt động và thông tin cho thuê.
* Máy chủ DHCP chính sẽ khởi tạo một kết nối cho mọi mối quan hệ chuyển đổi dự phòng DHCP được cấu hình trên máy chủ. Kết nối được sử dụng để đảm bảo thông tin thuê nhất quán trên cả hai máy chủ và cho phép mỗi máy chủ giám sát trạng thái hoạt động của đối tác. Máy chủ DHCP được thông báo nếu kết nối bị hỏng vì bất kỳ lý do gì. Để đảm bảo duy trì kết nối TCP liên tục giữa các đối tác chuyển đổi dự phòng DHCP, điều quan trọng là sử dụng địa chỉ IP tĩnh trên tất cả các giao diện mạng máy chủ DHCP. Nếu địa chỉ IP tĩnh của máy chủ DHCP cần được thay đổi, chẳng hạn như trong quá trình di chuyển DHCP, trước tiên bạn phải xóa tất cả các mối quan hệ chuyển đổi dự phòng DHCP tồn tại trên máy chủ đó, sau đó tạo lại các mối quan hệ khi địa chỉ IP mới đang hoạt động.



*Hình 2.11.3. DHCP Failover Comunication*

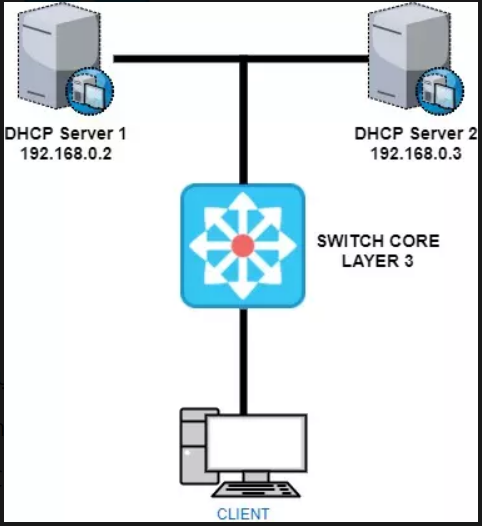
# **CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM**

## **Mục tiêu của mô hình ứng dụng**

Mô hình úng dụng giúp chúng ta thấy được tổng quan quá trình làm việc cách cấu hình máy chủ DHCP và cấu hình máy chủ DHCP Failover

Tạo ra một máy chủ DHCP để cáp phát tự động địa chỉ IPV4 cho các máy client và tạo ra máy chủ DHCP FailOver để tiếp tục cấp phát địa chỉ IPV4 khi một trong 2 máy chủ gặp vấn đề

## **Mô hình ứng dụng**



## **Yêu cầu thực hiện**

* Chuẩn bị 3 máy PC
* 2 máy chủ DHCP
* 1 máy Client

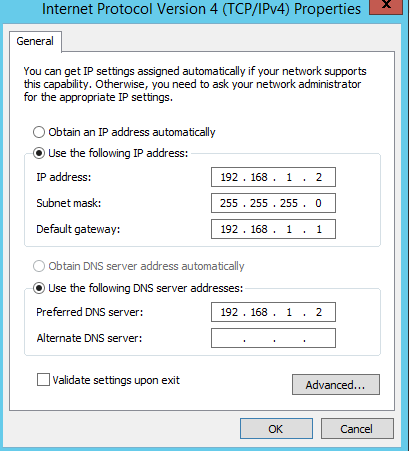
## **Các công cụ cần để thực hiện mô hình**

* Windows Server 2008
* Windows 10

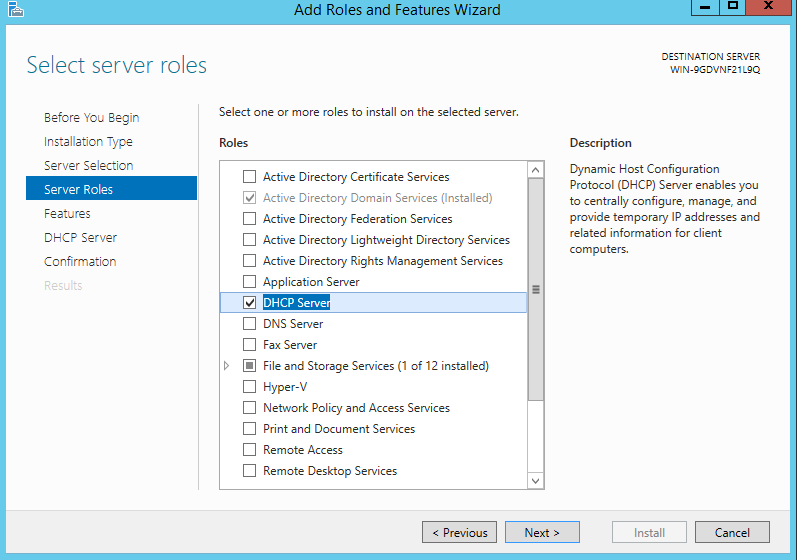
1. **Cài đặt DHCP**

- Cấu hình máy chủ DHCP để cấp phát địa chỉ IPV4.

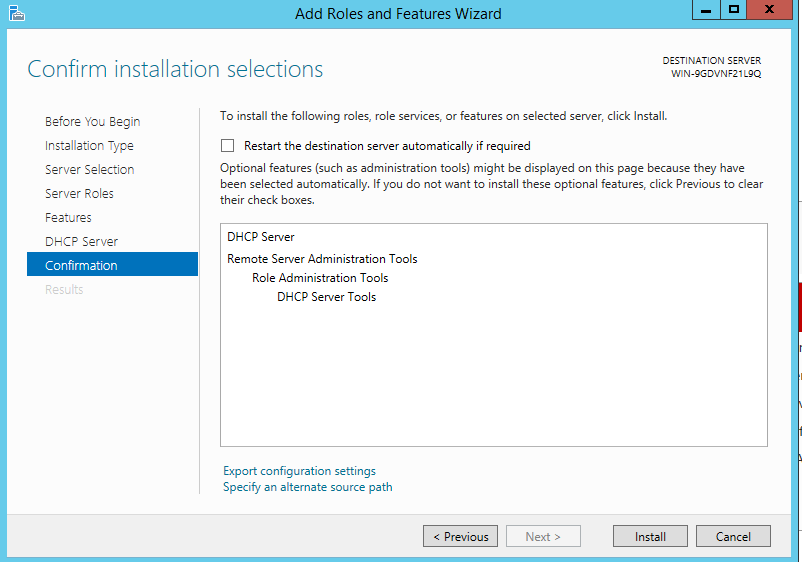
+ cấu hình ip cho máy chủ DHCP



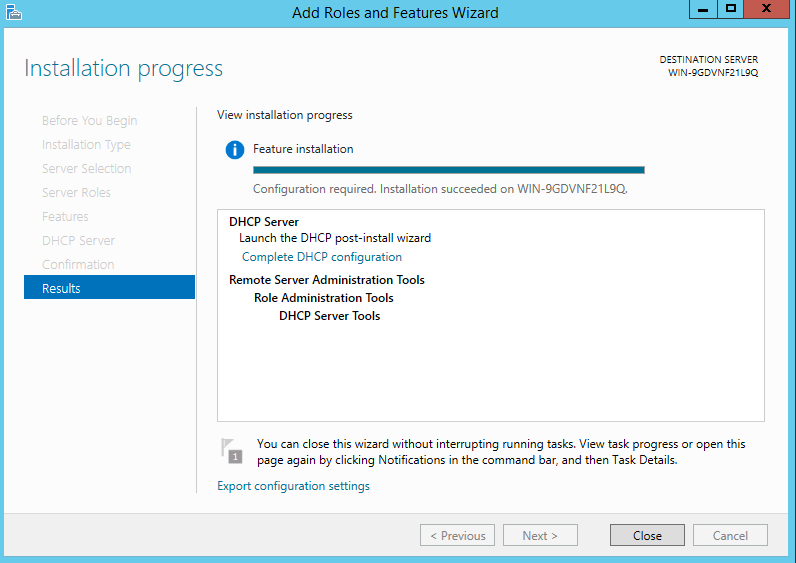
Add roles cho máy chủ DHCP.



Click chọn DHCP sever và ấn next cho tới muc cuối cùng.

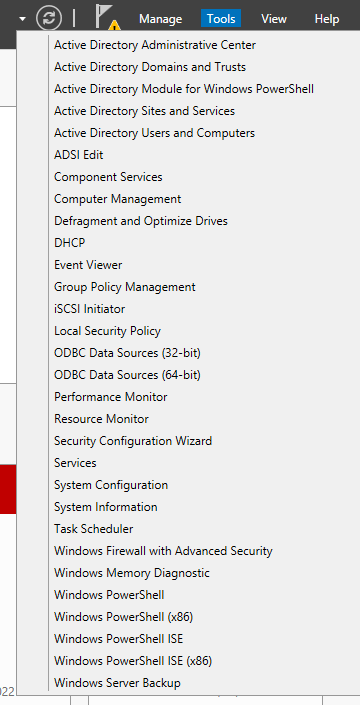


Chọn Install và đợi cài đặt xong.

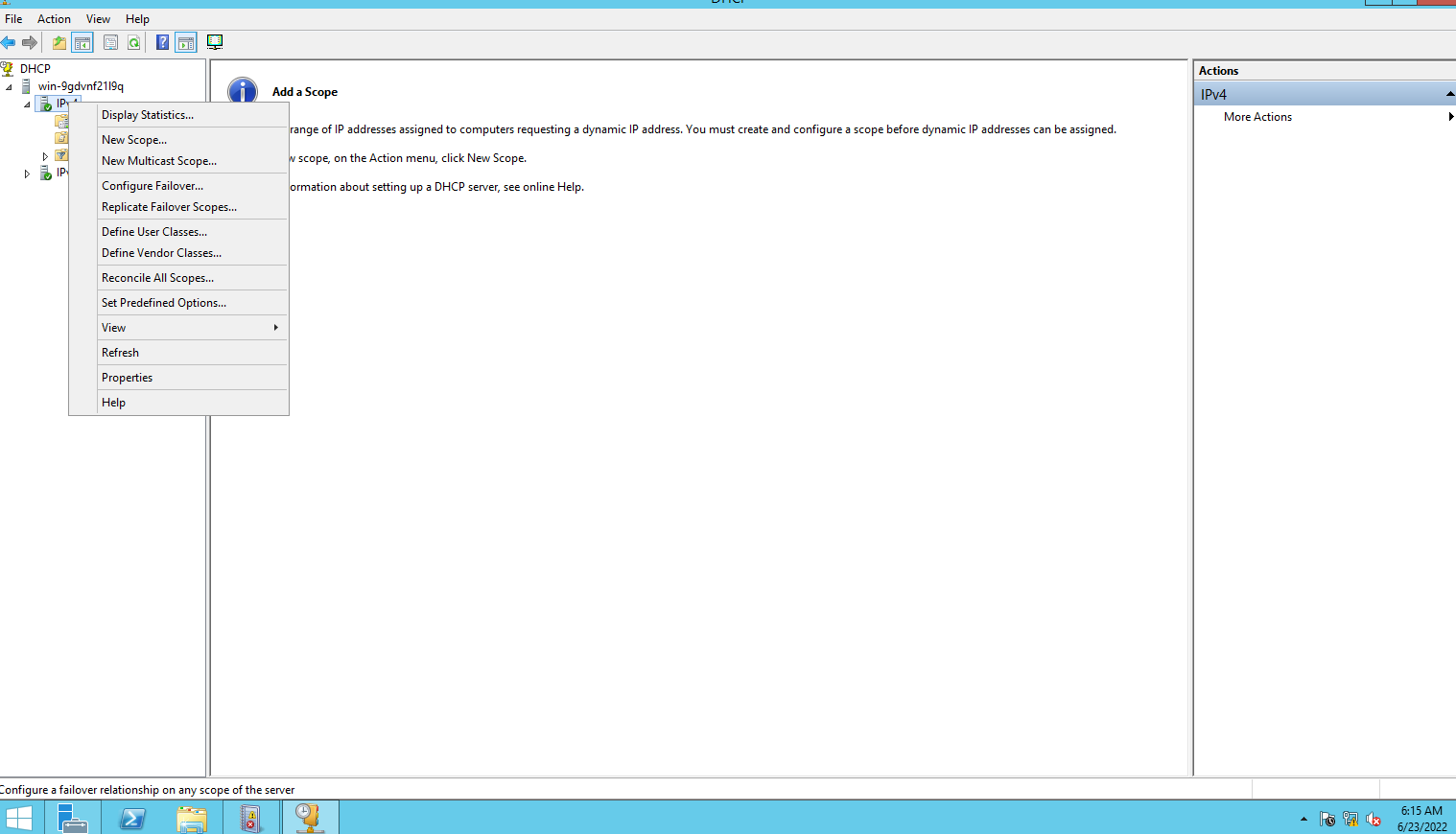


Sau khi cài đặt xong chúng ta chon Close.

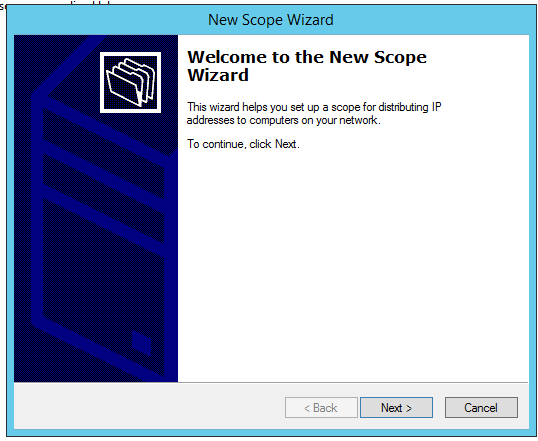
+ Cấu hình cho máy chủ DHCP.

****

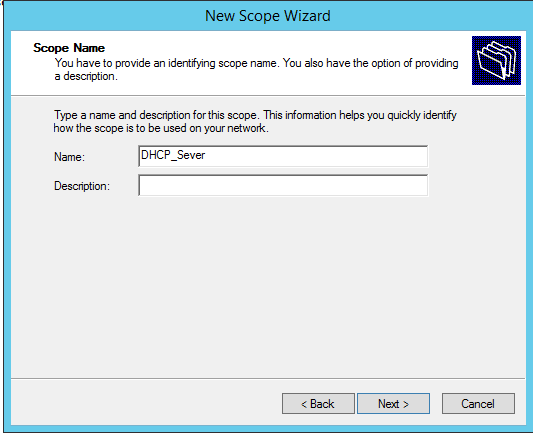
Chúng ta chon tools và click vào mục DHCP.



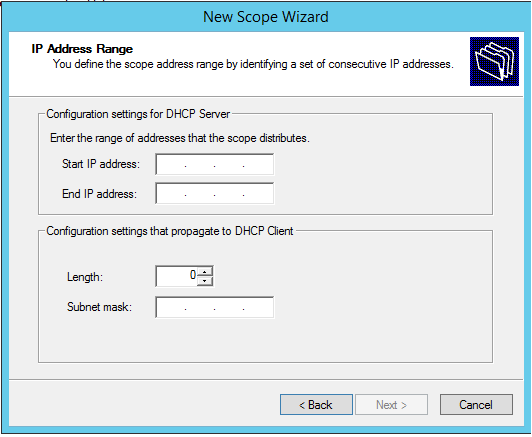
Sau đó chúng ta chuột trái vào IPV4 và chọn New Scope.



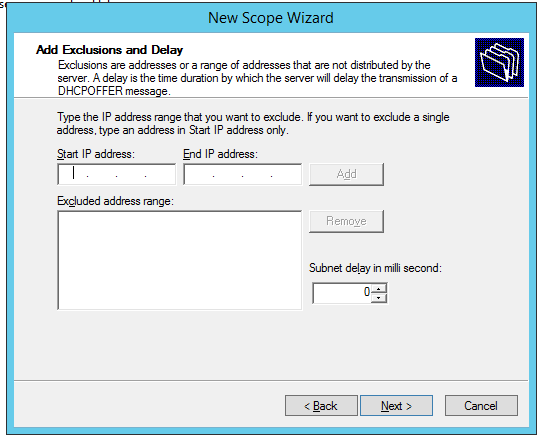
Tiếp theo chúng ta chọn Next.



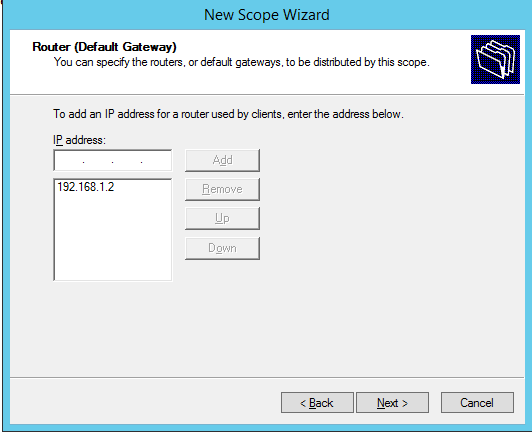
Xong chúng ta sẽ đặt tên cho máy chủ DHCP của mình.



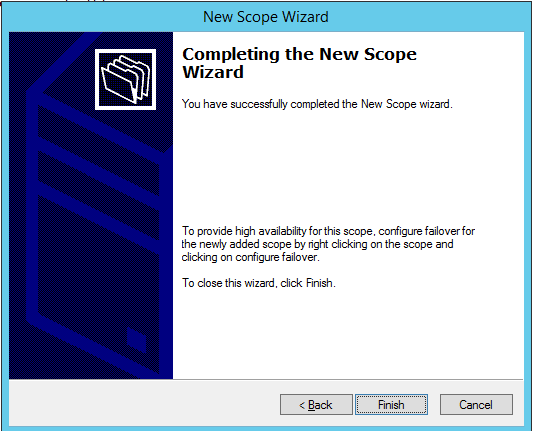
Ở mục này chúng ta sẽ điền cái vùng mà địa chỉ ipv4 được cấp phát.



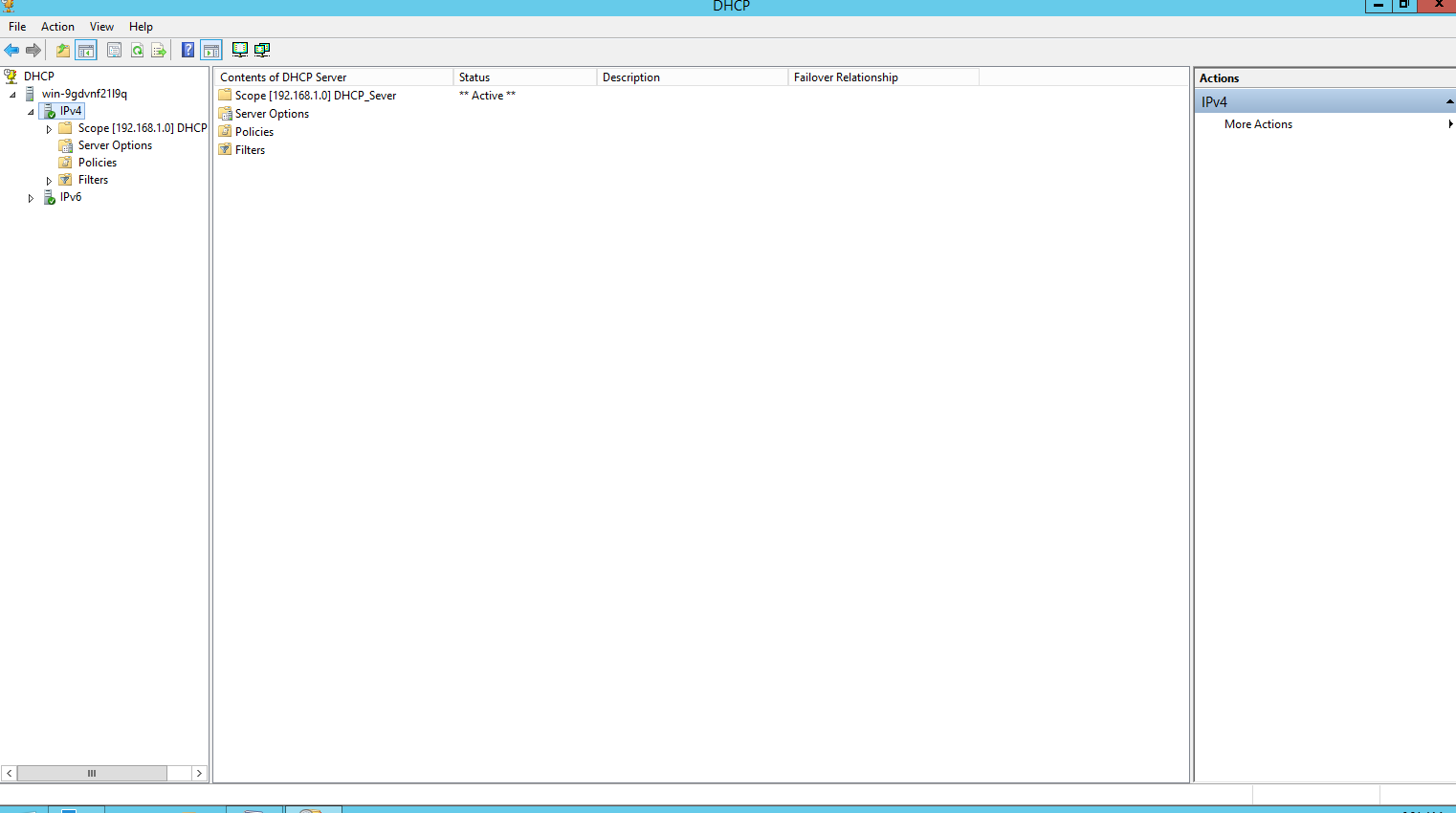
Mục này chúng ta sẽ nhập vùng ipv4 tĩnh mà được cấp phát sau đó chúng ta ấn next.



Mục này chúng ta sẽ nhập địa chỉ của máy chủ DHCP.

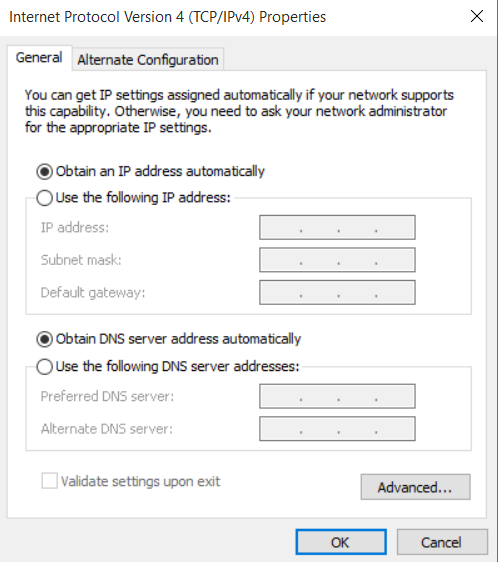


Sau đó chúng ta ấn next cho tới khi mục này chúng ta ấn Finish.

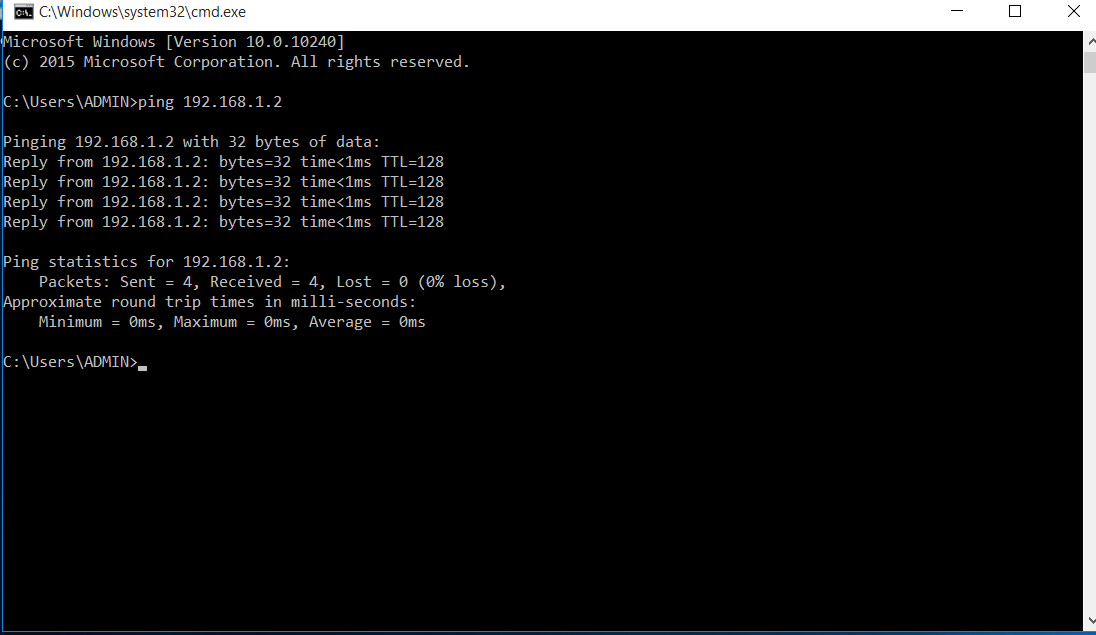


Vậy là chúng ta cấu hình xong máy chủ DHCP.

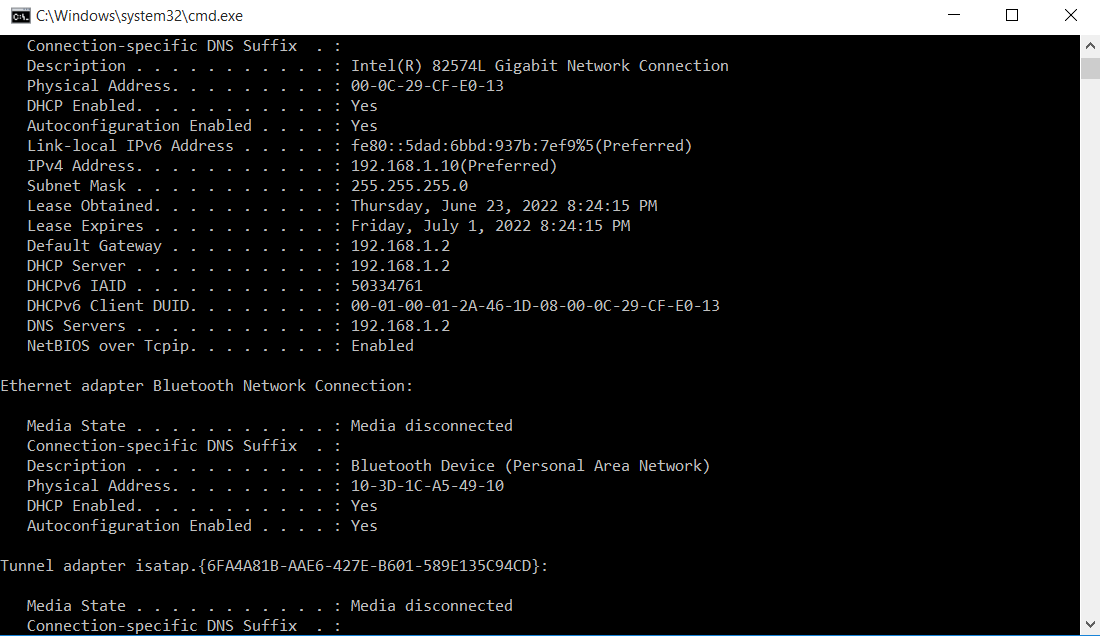
+ sau đó chúng ta sang máy client để cáu hình và kiểm tra xem đã được cấp phát địa chỉ hay chưa

****

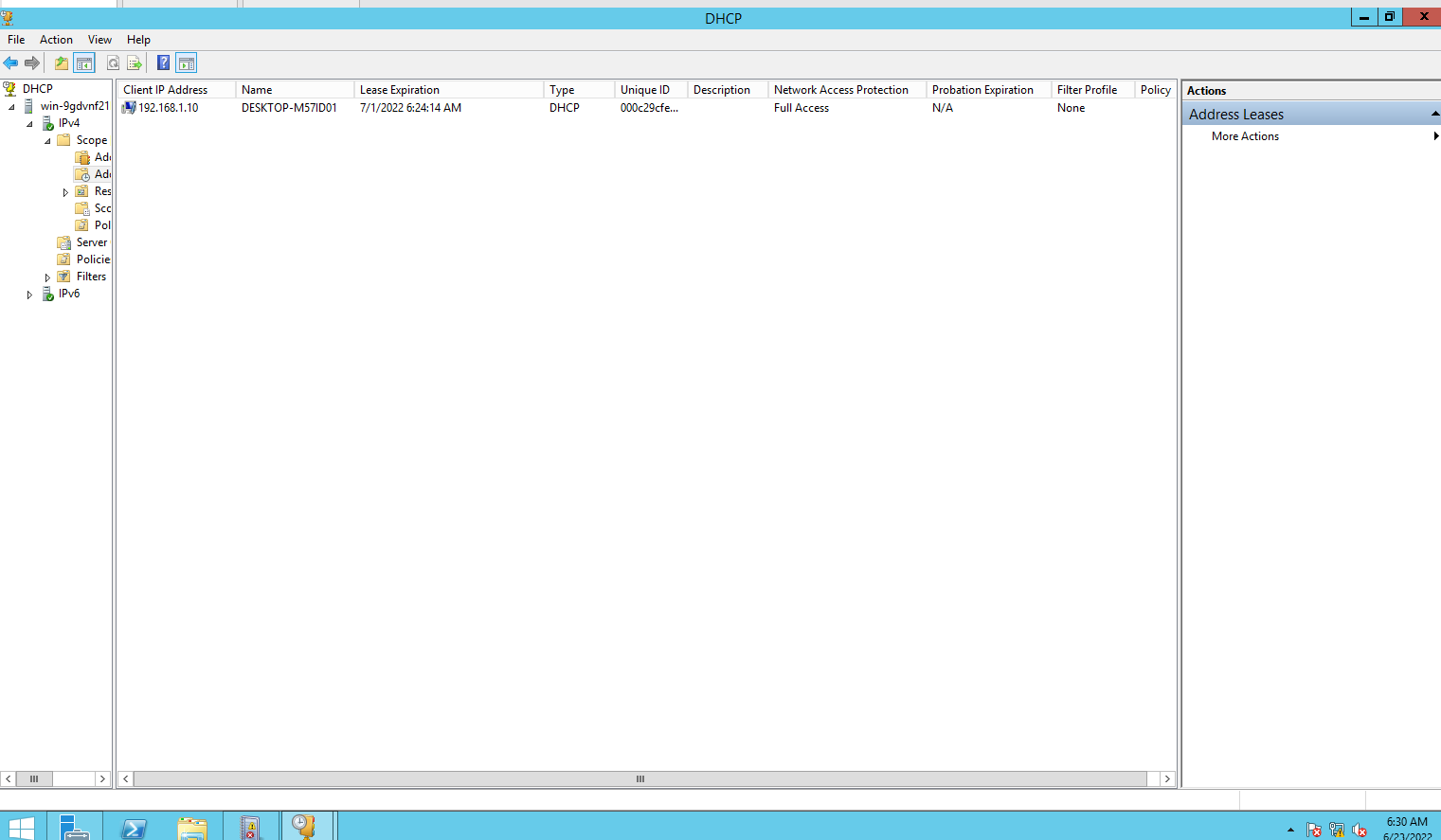
Ở máy client chúng ta chọn mục (Obtain an IP Address automatically) để máy nhận ip tự động.



Tiếp theo chúng ta mở cmd ở client lên và ping thử tới máy chủ DHCP hay chưa ở đây chúng ta thấy đã ping thành công.



Tiếp theo chúng ta gõ lênh ipconfig /all để kiểm tra xem máy client nhận ip từ máy chủ nào. Ở đây chúng ta thấy máy client nhận ip từ máy chủ DHCP Server là 192.168.1.2 chính là máy chủ chúng ta vừa cấu hình.

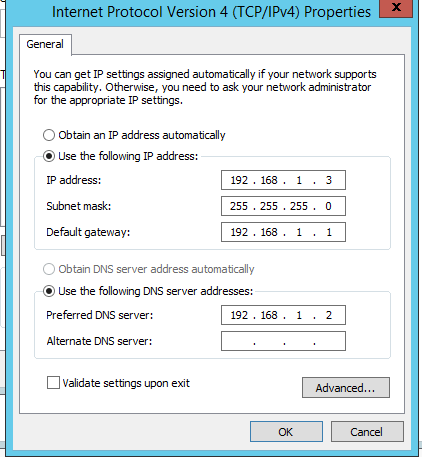


Sang máy chủ DHCP kiểm tra thì chúng ta thấy một địa chỉ IPV4 đã được cấp phát thành công.

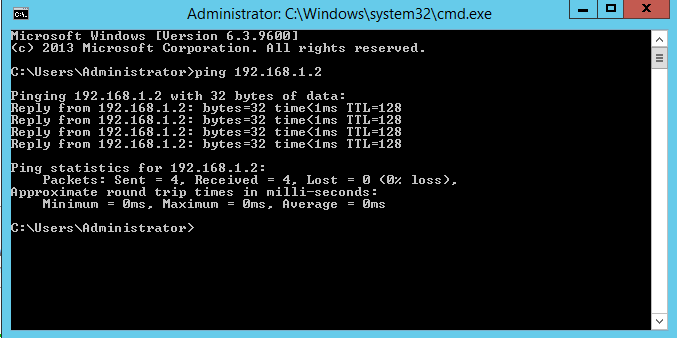
**+ Cấu hình máy chủ DHCP FailOver**

Ở máy chủ DHCP số 2 chúng ta cũng Add roles DHCP cho máy chủ.

Tiếp theo chúng ta cấu hình địa chỉ ip cho máy chủ DHCP số 2 và ping thử tới máy chủ DHCP có thành công hay không.

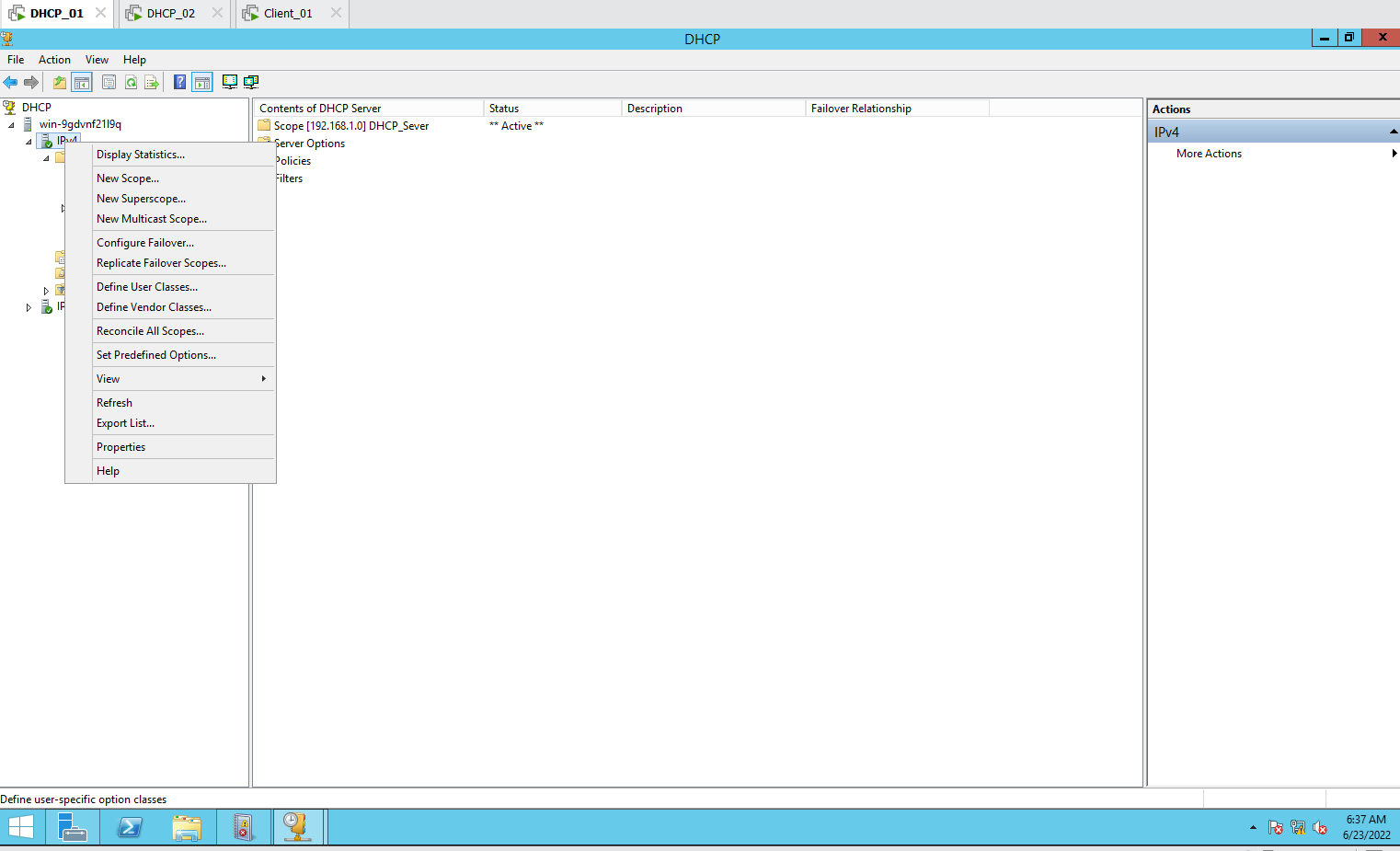


Cấu hình IP cho máy chủ DHCP số 2.

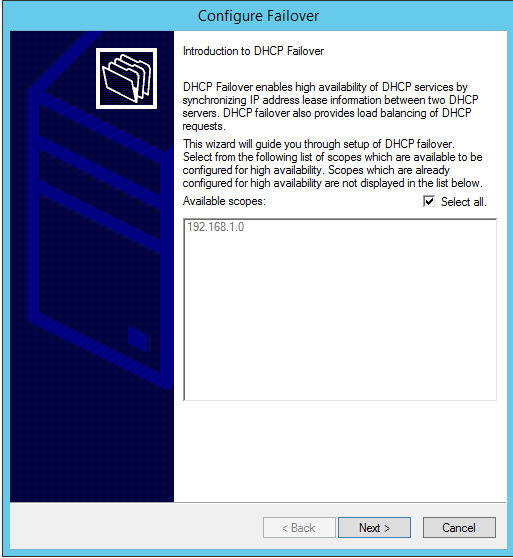


Ping thử tới máy chủ DHCP số 1 hay không ở đây ta đã ping thành công.

+ Sau đó chúng ta sang máy chủ DHCP số 1 để cấu hình DHCP Failover.



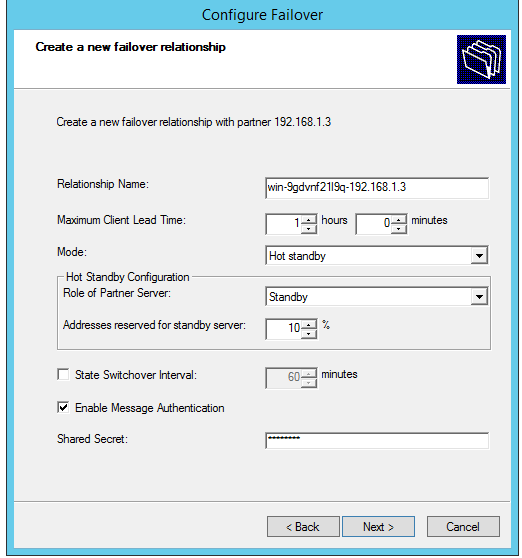
Chúng ta vào lại mục cấu hình DHCP của máy chủ số 1 và chuột phải vào IPV4 chọn mục Configure Failover.



Ở mục này chúng ta chọn next.



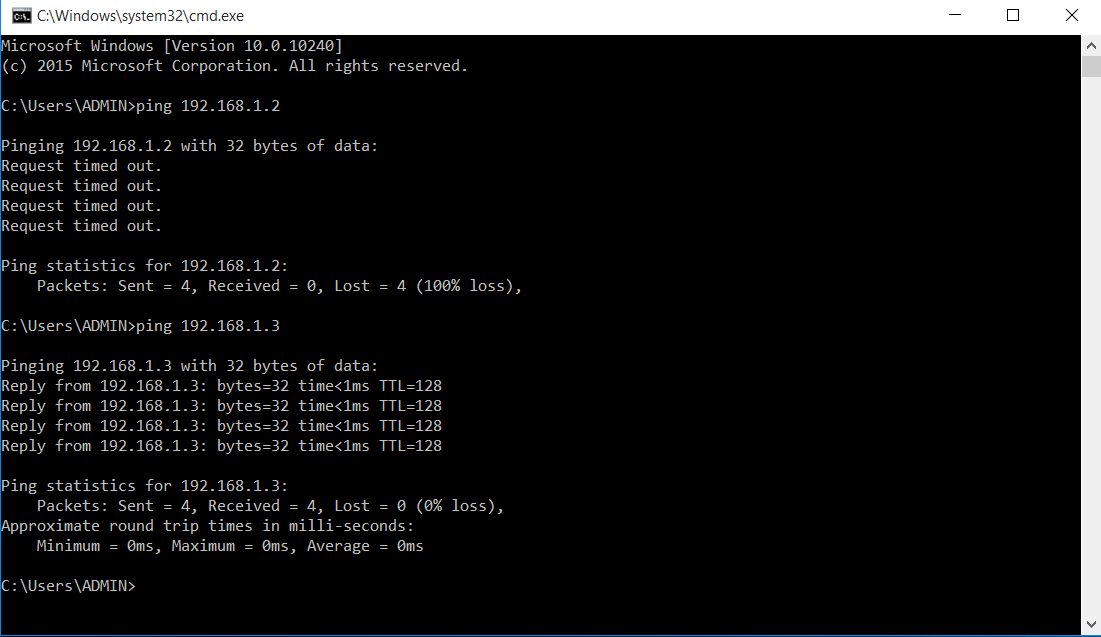
Ở mục này chúng ta nhập địa chỉ ip của máy chủ DHCP số 2.



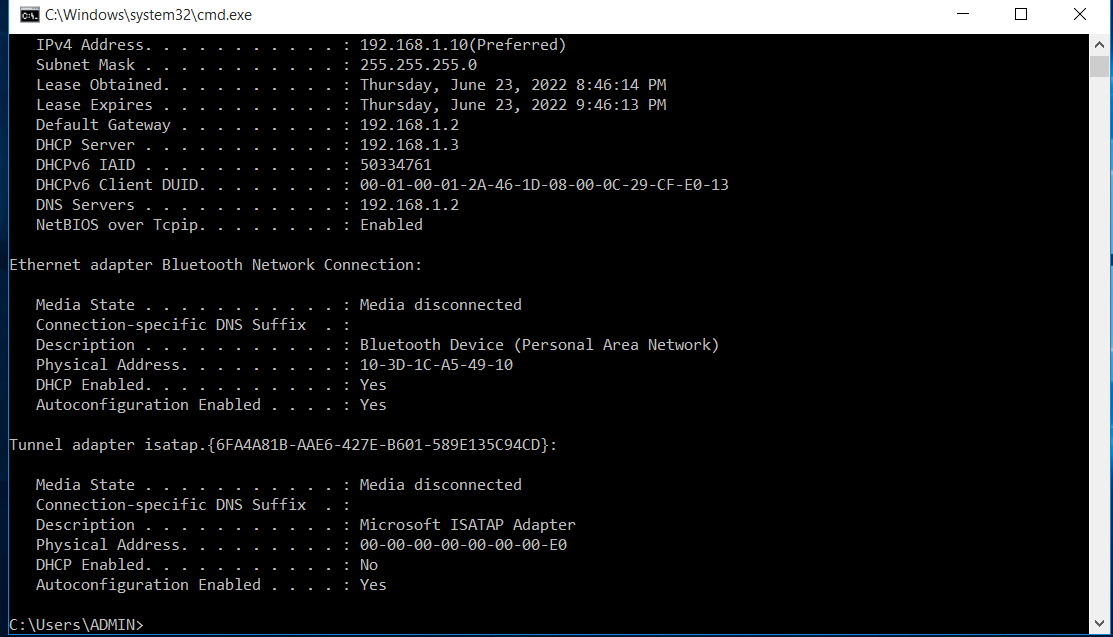
Ở mục này chúng ta nhập các thông số yêu cầu và ô cuối cùng chúng ta sẽ nhập pass mà chúng ta muốn.

Sau đó chúng ta ấn next cho tới khi hoàn thành

Sau đó chúng ta tắt máy chủ DHCP số một và sang máy client kiểm tra xem máy chủ DHCP số 2 có hoạt động hay không sau khi máy chủ DHCP số 1 sập.



Ở máy client chúng ta ping tới máy chủ số 1 và không thành công do ta đã tắt máy chủ số 1 rồi. Sau đó chúng ta ping thử tới máy chủ số 2 thì đã thành công.



Sau đó chúng ta gõ lệnh ipconfig /all để xem máy chủ nào đang cấp phát ip cho máy client như trên hình ta thấy máy chủ DHCP đang cấp phát ip đó 192.168.1.3 là ip của máy chủ DHCP số 2 vậy là chúng ta đã cấu hình xong máy chủ DHCP và DHCP FailOver.

## **Tấn công máy chủ DHCP bằng YERSINIA**

* + *Các công cụ cài đặt*

+Một máy Client chạy OS LINUX để sự dung công cụ Yersinia để tấn công.

+ Hai máy Client chạy Windows để xem thử sau khi bị tấn công có thể truy cập vào máy chủ hay không.

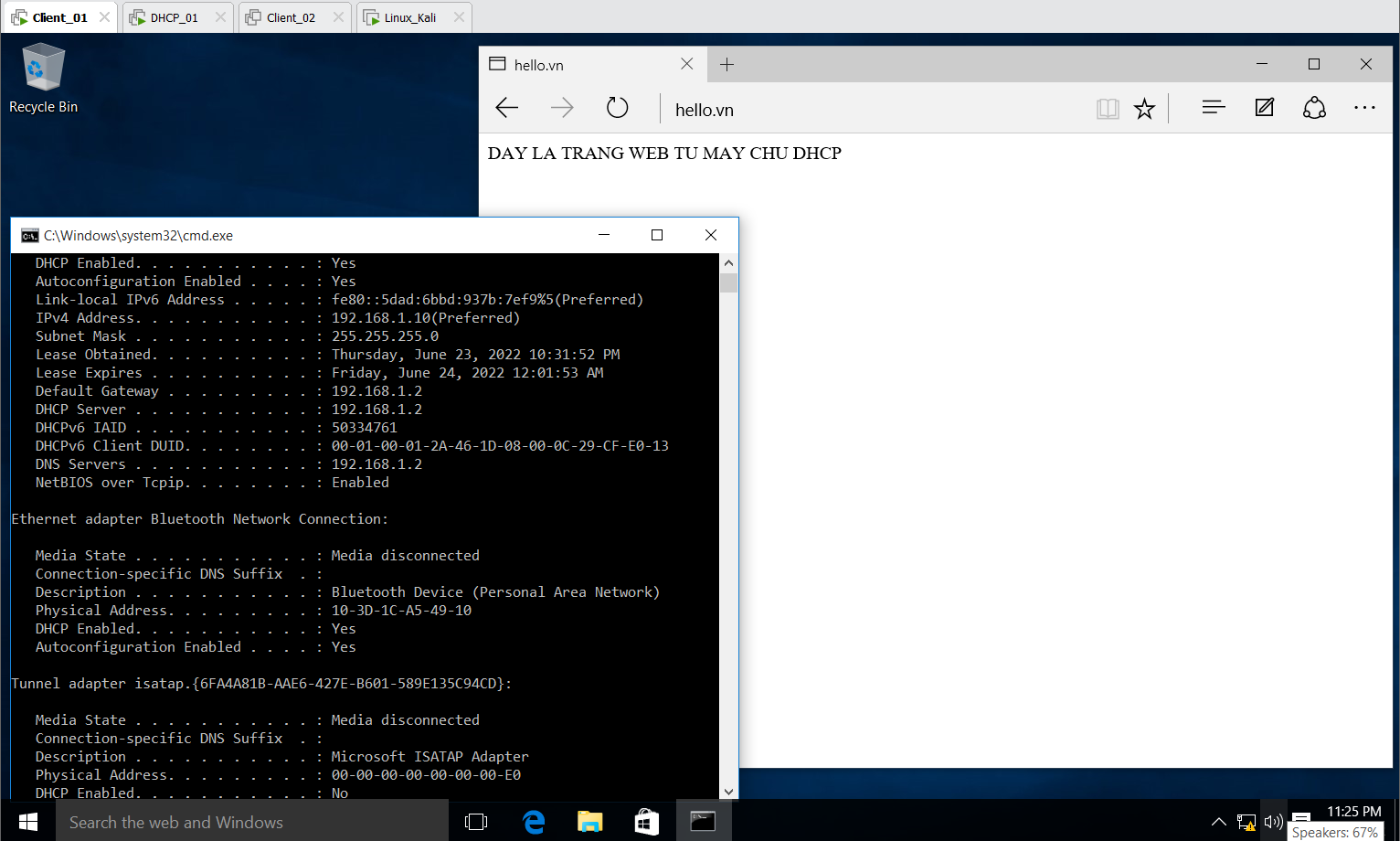
+ Một máy chủ DHCP có cài tên miền DNS và có Web Sever để test truy cập.

* + *Cách thức tấn công:*

Như chung ta đã biết máy chủ DHCP là một máy chủ cung cấp địa chỉ IPV4 cho các máy con trong mạng và số địa chỉ mà có thể cung cấp là hữu hạn vậy nên chúng ta sẽ tấn công vào máy chủ bằng cách liên tục giả mạo các máy con xin cấp phát địa chỉ IP để chiểm hết các điện chỉ mà máy chủ có bằng cách liên tục gửi các gói tin DISCOVER. làm cho các máy truy cập sau không được cấp phát IP.

* + *Kiểm tra:*

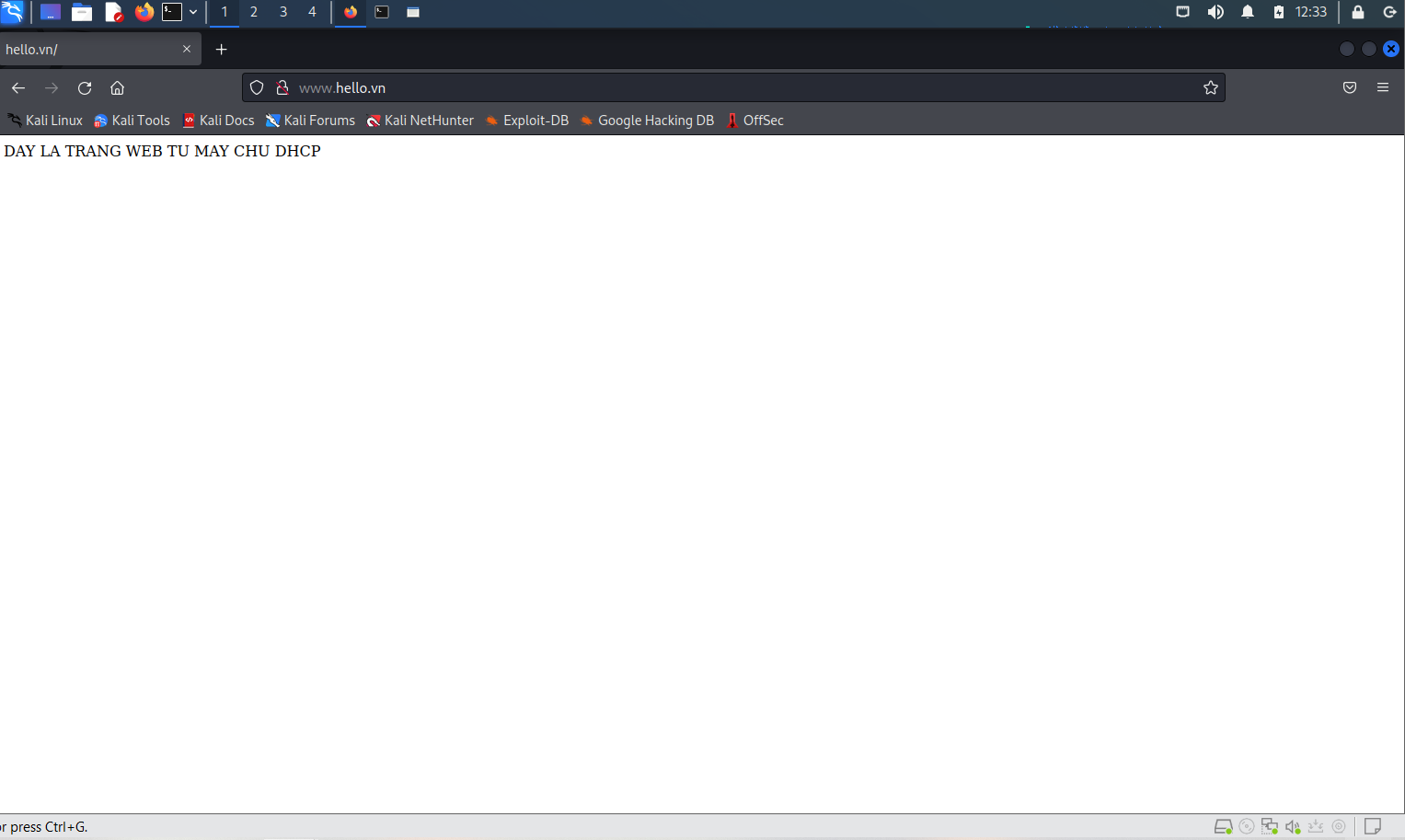
+ Kiểm tra xem máy chủ DHCP có hoạt động bình thường không bằng cách chúng ta dùng máy client truy cập tới trang web mà chúng ta đã cài đặt và xem máy chủ DHCP có cấp phát địa chỉ IPV4 cho máy client hay không.



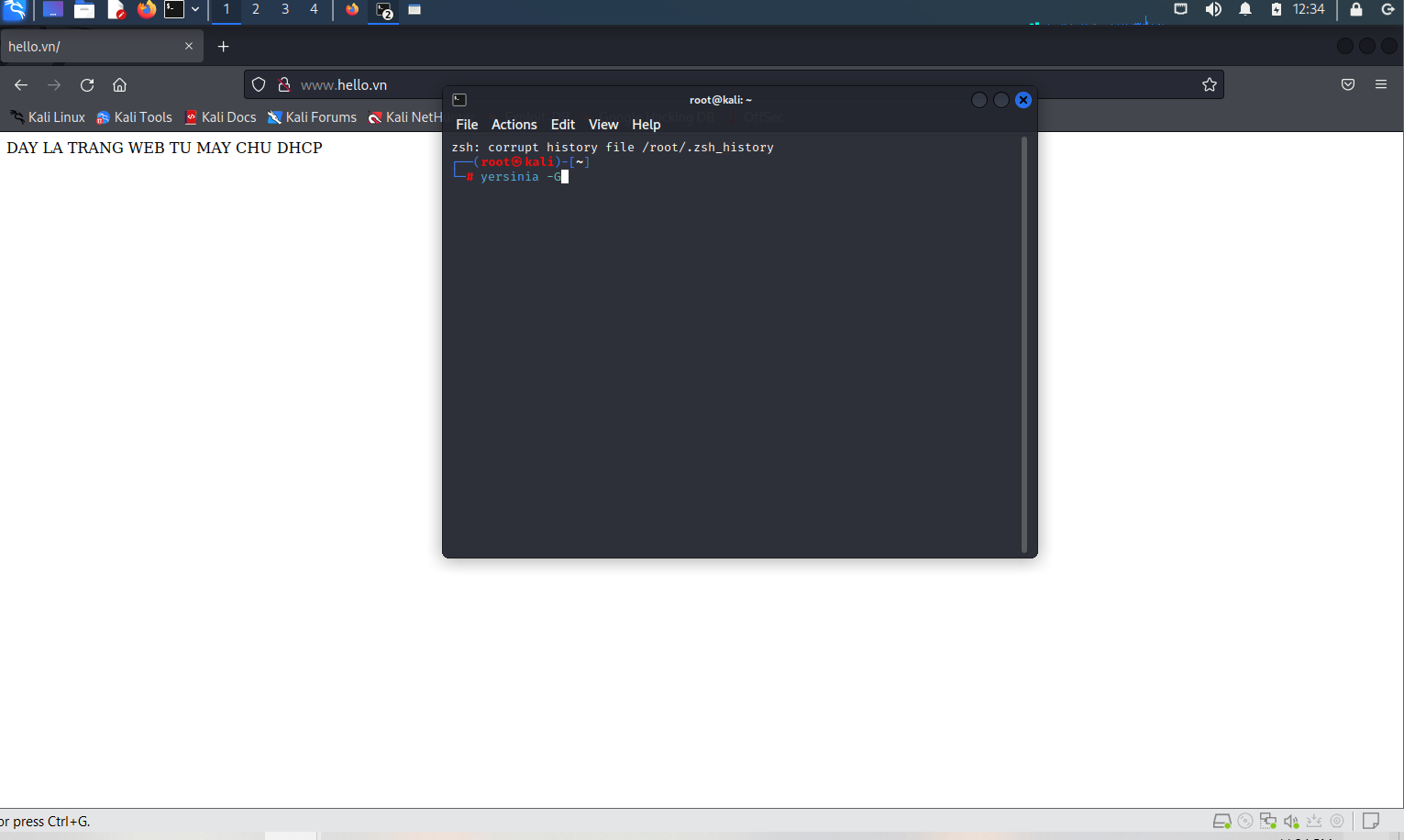
Ở đây ta thấy máy Client vẫn truy cập tới máy chủ bình thường.

* + *Tấn công:*

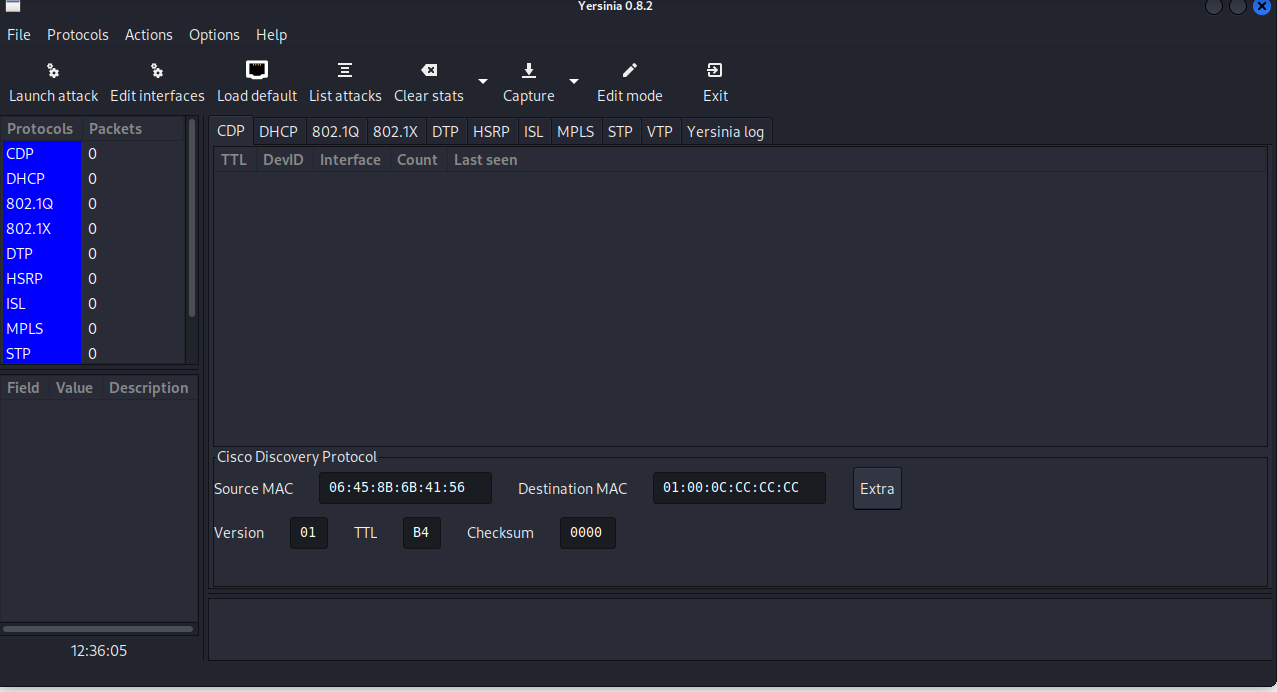
Kiểm tra xem máy Linux có kết nối tới máy chủ DHCP không.



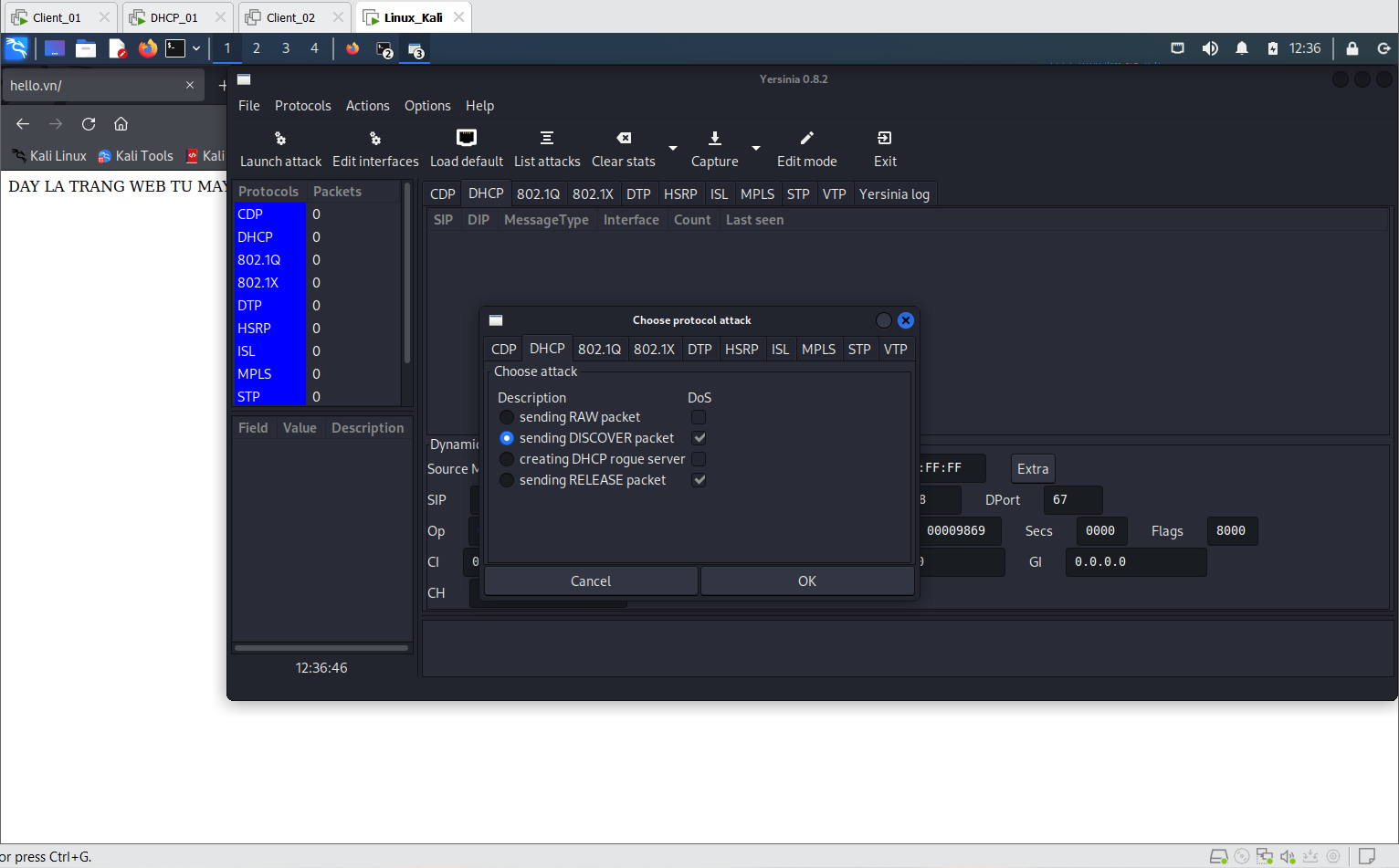
Như hình ta thấy máy Linux truy cập máy chủ DHCP bình thường và sau đây ta tiến hành tấn công làm đầy Port.



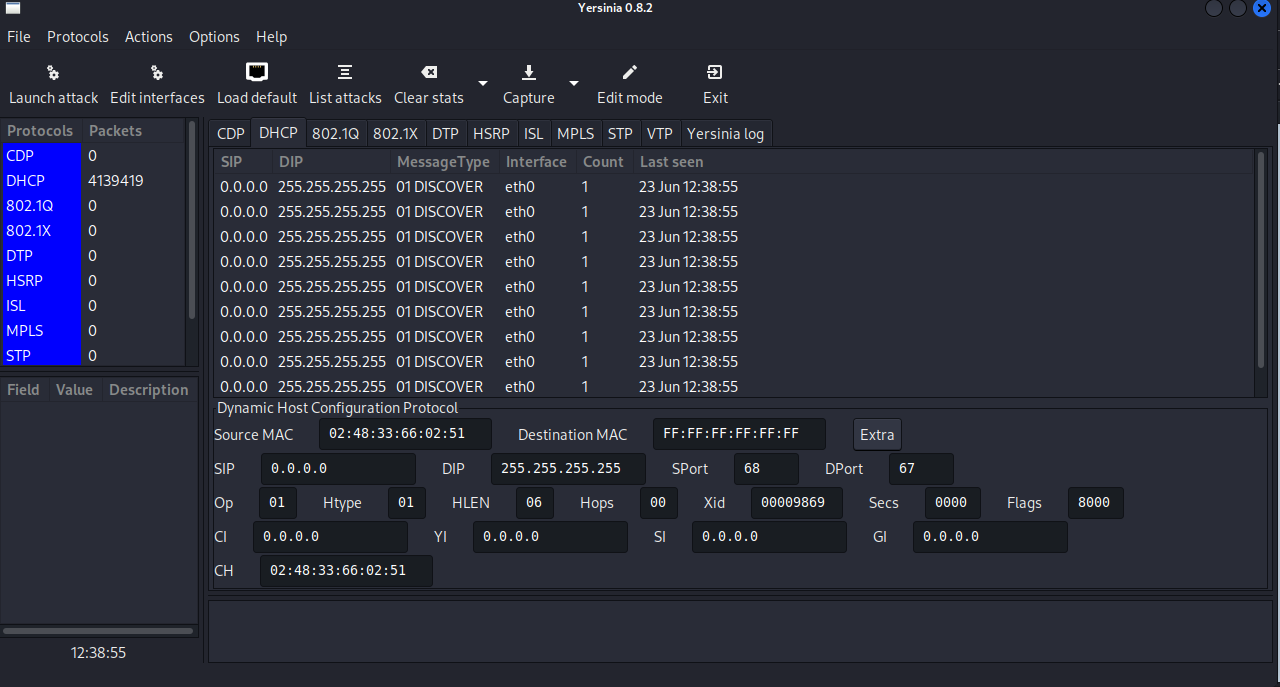
Ta mở cmd của Linux lên và gõ lệnh Yersinia - G để mở tool lên (cách cài Yersinia các bạn có thể tự tìm hiểu trên mạng).



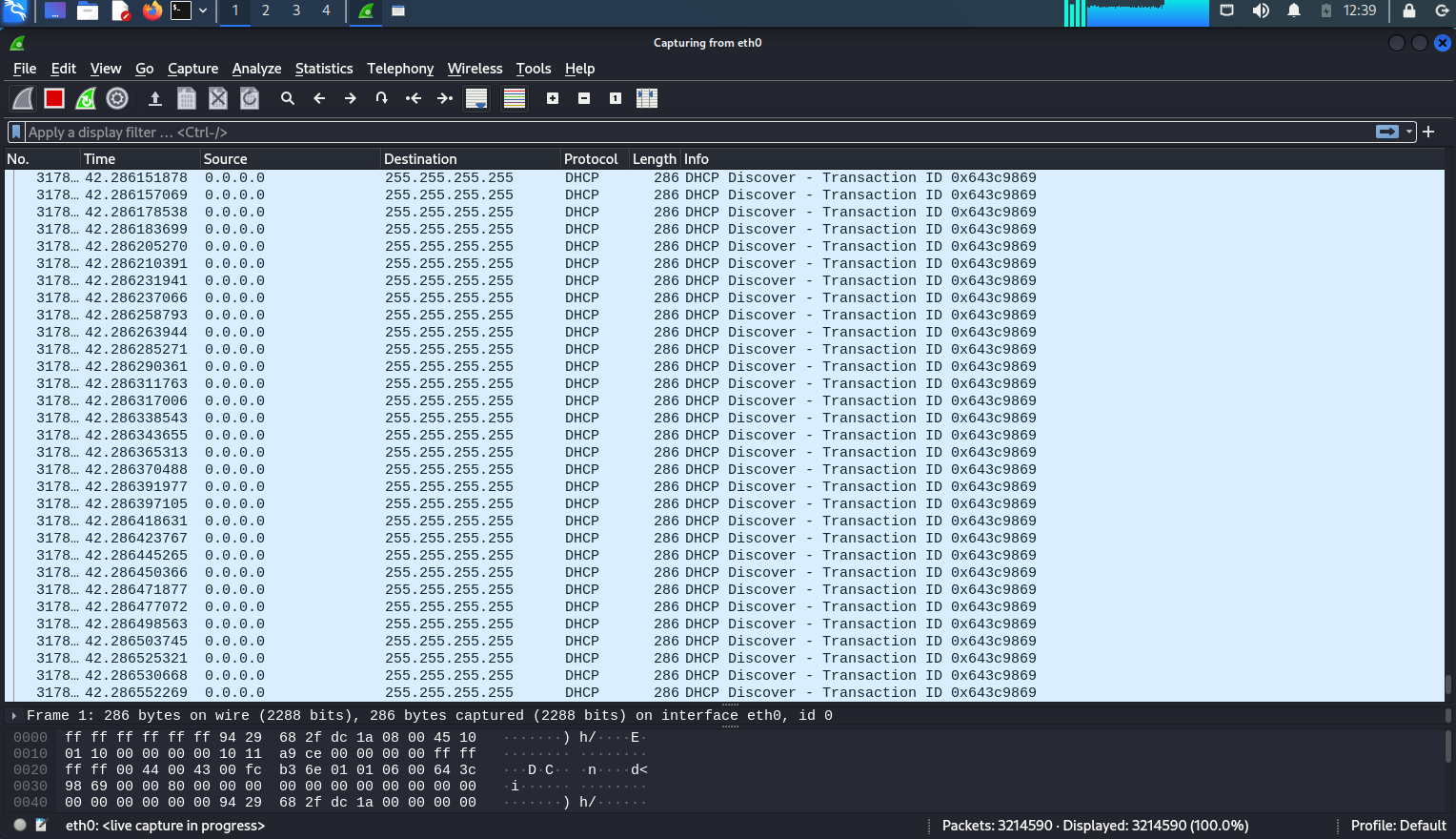
Ở đây ta chọn DCHP



Sau đó chúng ta chọn Launch Attack và chọn Sending Discover Packet và ấn OK.



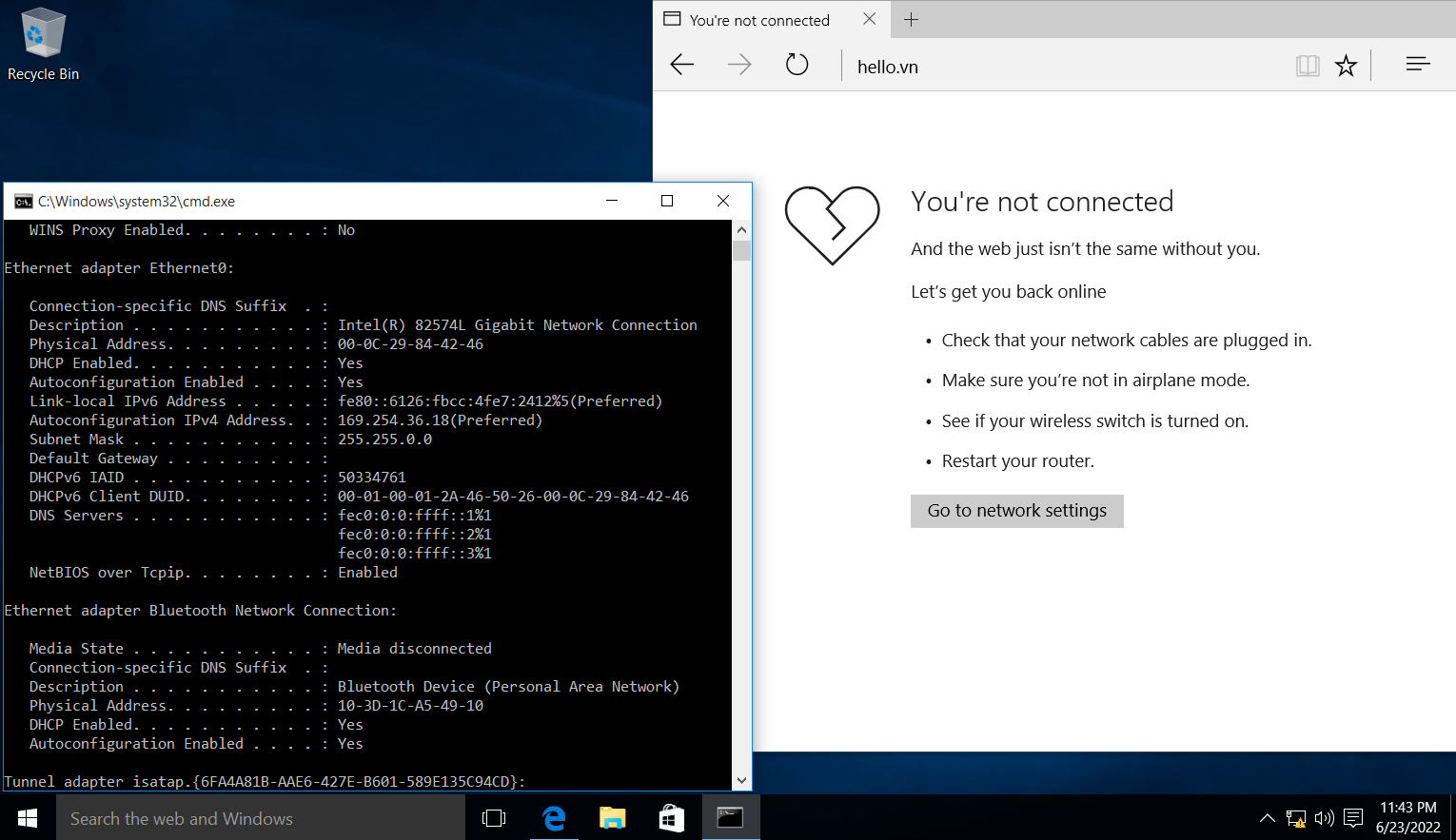
Sau đó liên tục các gói tin sẽ được gửi tới Server để tấn công chúng ta có thể mở Wireshark để xem cá gói tin được gửi đi.



Đây là các gói tin tấn công được gửi đi mà Wireshark bắt được.

* + *Kiểm tra tấn công có thành công hay không*

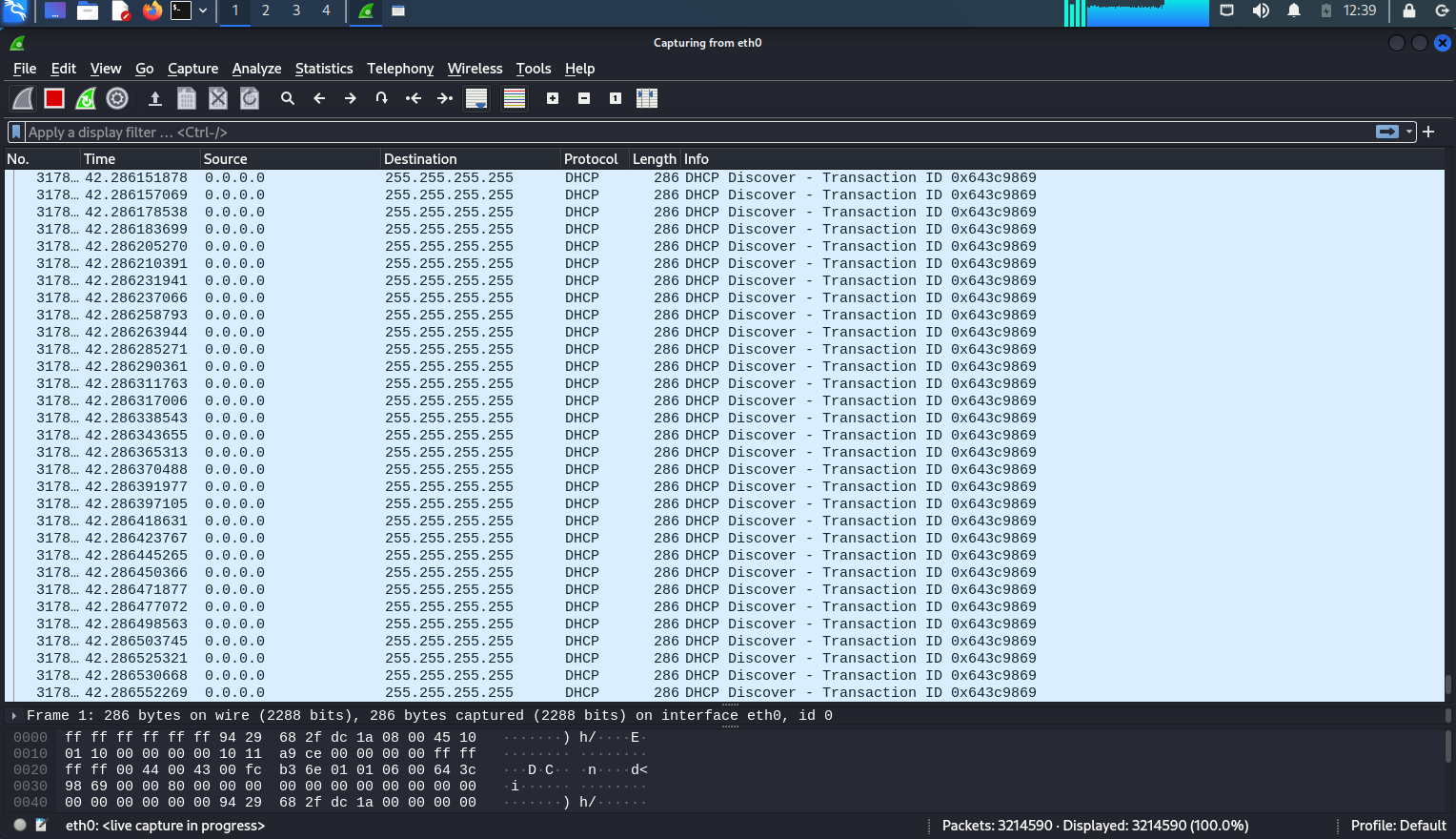
Chúng ta mở một máy Client khác lên và thử xin cấp phát địa chỉ IP từ Server được không.

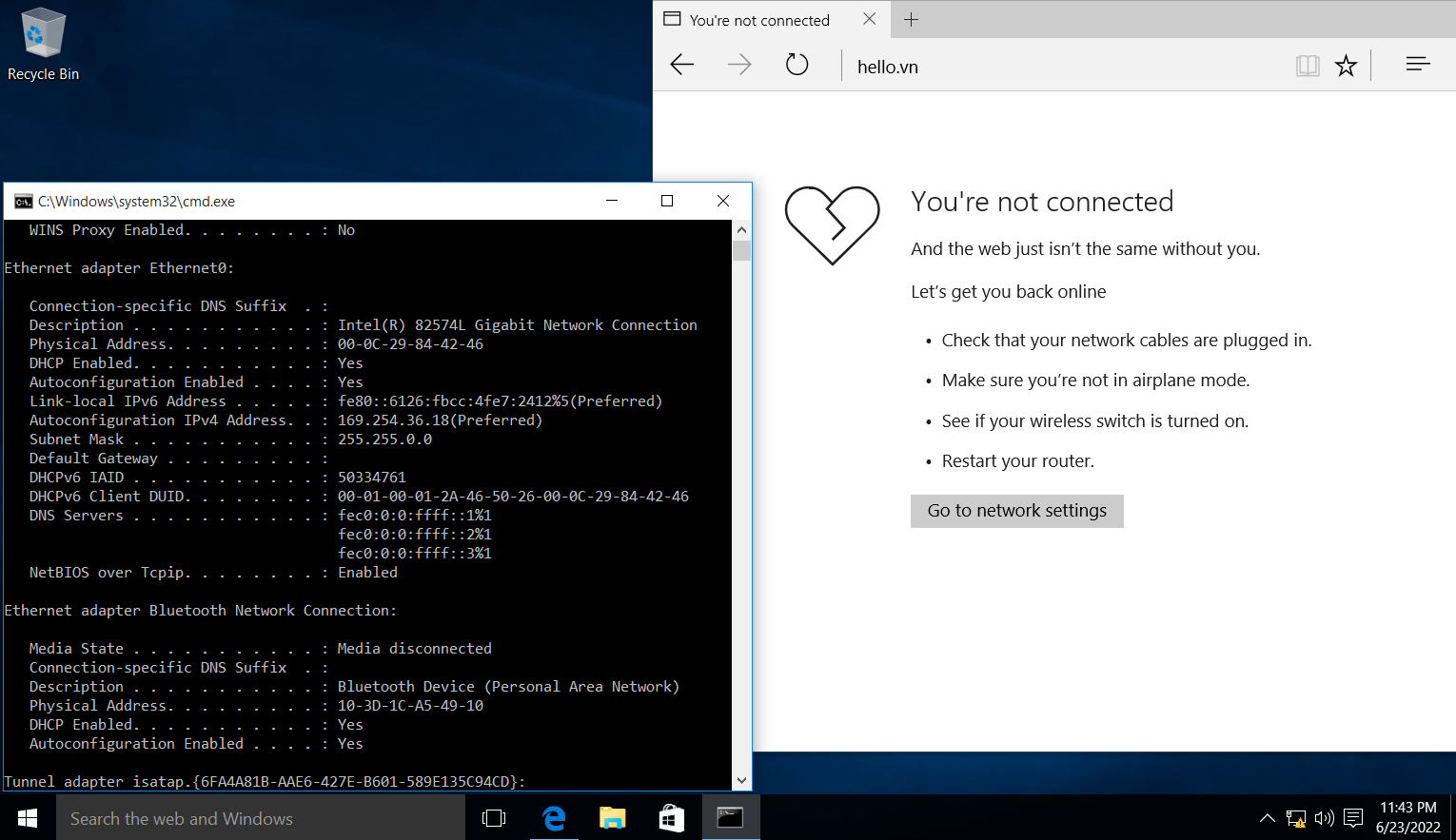


Kết quả chúng ta có thể thấy khi một máy Client mới xin truy cập cấp phát địa chỉ IP từ máy chủ DHCP thì không được nữa tại vì máy chủ đang bị tấn công và hiện tại không còn địa chỉ cho nó nữa.

* + *Kết quả*

Biết cách tấn công một máy chủ DHCP đơn giản để thử nghiệm trang Web của mình.





# **CHƯƠNG 4. KẾT LUẬN VÀ HƯỚNG VÀ PHÁT TRIỂN**

* **Kết luận**
* Nằm được phương pháp xây dựng được một máy chủ DHCP đơn giản. Nắm được kiến thức xây dựng một máy chủ và điều hành một máy chủ DHCP.
* Hiểu và biết cách vẫn dụng vào việc phòng ngừa tấn công máy chủ DHCP và hạn chế những đợt tấn công không mong muốn.
* Thông qua việc học tập và hưỡng dẫn của thầy về máy chủ DHCP, chúng em bước đầu đã xây dựng được một máy chủ DHCP đơn giản để cấp phát các địa chỉ IPV4 cho các máy client để phát triển lên các máy sever hoản chỉnh hơn. Hệ thông đạt được được các chưng năng cơ bản của một máy chủ DHCP
* **Hướng Phát Triển**
* Tìm hiểu thêm về máy chủ DHCP để nâng cấp hơn để cấp phát nhiều địa chỉ hơn.
* tìm hiểu thêm các phần mềm chống dos và ddos làm cho hệ thống máy chủ DHCP bị đầy các port.
* tìm hiểu và tiếp tục phát triển các chức năng nâng cao hơn.

# TÀI LIỆU THAM KHẢO

[1]<https://www.wikiwand.com/vi/DHCP>

[2] <https://tailieuthamkhao.org/bai-giang-dich-vu-dhcp-dynamic-host-configuation-protocol-1348/>

[3] <https://www.totolink.vn/article/111-dhcp-la-gi-tim-hieu-ve-dhcp.html>

[4] <https://viblo.asia/p/cau-hinh-dhcp-failover-multi-vlan-tren-windows-server-2016-63vKjn2kK2R>

[5] <https://viettelco.vn/huong-dan-cau-hinh-dhcp-failover-tren-windows-server/>