TẠP CHÍ KHOA HỌC TRƯỜNG ĐẠI HỌC HOA LƯ
ISSN 2615-9538
Website: http://hluv.edu.vn/vi/tckh

NGHIÊN CỨU VLAN, TRUNK, DHCP, NAT VÀ ỨNG DỤNG THỰC HÀNH LAB TRÊN PHẦN MỀM GIẢ LẬP EVE-NG

Nguyễn Tất Thắng[1]

Ngày nhận bài: 11/4/2024 Ngày chấp nhận đăng: 20/6/2024

Tóm tắt: *Bài viết nghiên cứu các khái niệm VLAN, TRUNK, DHCP và NAT trong lĩnh vực mạng máy tính, trên cơ sở đó tác giả đã tiến hành thực nghiệm thông qua bài Lab trên phần mềm giả lập EVE-NG. VLAN được tìm hiểu như một công nghệ cho phép chia mạng vật lý thành nhiều mạng logic độc lập; TRUNK là kết nối cho phép truyền dữ liệu giữa các VLAN trên các thiết bị mạng; DHCP là giao thức quản lý và cấp phát địa chỉ IP tự động; NAT là kỹ thuật chuyển đổi địa chỉ IP và cổng. Thực hành trên phần mềm EVE-NG giúp chúng tôi làm quen với các bước cấu hình và quản lý các tính năng này trên các thiết bị mạng như Switch và Router. Qua đó, chúng tôi có cơ hội áp dụng những kiến thức học được vào các tình huống thực tế, từ việc thiết kế, cấu hình thiết bị đến việc kết nối với Internet. Bài viết mang lại lợi ích cho những người học và nghiên cứu mạng máy tính, giúp họ nắm vững lý thuyết và kỹ năng thực hành cần thiết.*

Từ khóa: *VLAN, TRUNK, DHCP, NAT*

RESEARCH VLAN, TRUNK, DHCP, NAT AND PRACTICE LAB APPLICATIONS ON EVE-NG EMULATION SOFTWARE

Abstract: *The article studies the concepts of VLAN, TRUNK, DHCP and NAT in the field of computer networks, based on which the author conducted experiments through a Lab on EVE-NG simulation software. VLAN is understood as a technology that allows the physical network to be divided into many independent logical networks; TRUNK is a connection that allows data to be transferred between VLANs on network devices; DHCP is an automatic IP address allocation and management protocol; NAT is a technique for converting IP addresses and ports. Practicing on EVE-NG software helps us become familiar with the steps to configure and manage these features on network devices such as switches and routers. Thereby, we have the opportunity to apply the knowledge we have learned to real situations, from designing and configuring devices to connecting to the Internet. The article benefits those who study and research computer networks, helping them master the theory and necessary practical skills.*

Keywords: *VLAN, TRUNK, DHCP, NAT*

1. Giới thiệu

Trong cuộc sống hiện nay, chúng ta có thể thấy kỹ thuật và công nghệ mạng có ý nghĩa vô cùng to lớn cho bất cứ doanh nghiệp, tổ chức hay cá nhân nào muốn quản lý tốt dữ liệu nội bộ hay muốn có đường truyền kết nối ổn định đều phải thông qua chúng. Trong đó kỹ thuật VLAN, TRUNK, DHCP, NAT sẽ không thể thiếu cho các doanh nghiệp, tổ chức hay cá nhân triển khai trên hệ thống mạng LAN của mình.

[1] Khoa Ngoại ngữ - Công nghệ thông tin, Trường Đại học Hoa Lư.

Trong mạng LAN, router thường đóng vai trò phân tách các mạng LAN khác nhau, thường dựa trên địa chỉ IP, để cho phép trao đổi dữ liệu giữa các mạng LAN khác nhau. Router là thiết bị phân cấp mạng cao hơn, giúp kết nối các mạng khác nhau và quyết định định tuyến dữ liệu. Còn trong VLAN, switch đóng vai trò quan trọng trong việc phân tách các mạng con ảo (VLANs) trong một mạng LAN vật lý. Switch quản lý việc gán các cổng vào từng VLAN, đảm bảo rằng các thiết bị trong cùng một VLAN có thể trao đổi dữ liệu mà không ảnh hưởng đến các VLAN khác. Việc tạo lập nhiều VLAN trong cùng một mạng LAN (*giữa các khoa trong một trường học, giữa các phòng trong một công ty,...*) giúp giảm thiểu miền quảng bá (*broadcast domain*) cũng như tạo thuận lợi cho việc quản lý một mạng cục bộ rộng lớn. Nhờ đó mà các máy tính trong mạng có thể chia sẻ tài nguyên, chia sẻ phần mềm, có tính linh động cao, thắt chặt vấn đề an ninh mạng và tiết kiệm được tài nguyên phần cứng.

Dịch vụ DHCP mang đến nhiều tiện ích cho người dùng trong quá trình quản trị cấu hình mạng TCP/IP, giảm được các tình trạng lỗi IP như gán trùng, gán sai địa chỉ,… Sự xung đột IP sẽ được hạn chế tối đa. Kỹ thuật NAT giúp che giấu IP bên trong mạng LAN, có thể chia sẻ kết nối internet cho nhiều máy tính, thiết bị di động khác nhau trong mạng LAN chỉ với một địa chỉ IP public duy nhất, giúp nhà quản trị mạng lọc được các gói tin đến và xét duyệt quyền truy cập của IP public đến 1 port bất kỳ.

Trong phạm vi bài viết này tác giả tập trung trình bày những nghiên cứu cơ bản về VLAN, TRUNK, DHCP, NAT và ứng dụng cấu hình Lab trên phần mềm giả lập EVE-NG.

2. Nội dung

2.1. VLAN

VLAN (*Virtual Local Area Network*) là kỹ thuật được sử dụng trên Switch, dùng để chia một Switch vật lý thành nhiều Switch luận lý. Mỗi một Switch luận lý gọi là một Vlan hoặc có thể hiểu Vlan là một tập hợp của các cổng trên Switch nằm trong cùng miền quảng bá. Các cổng trên Switch có thể được nhóm vào các Vlan khác nhau trên một Switch hoặc được triển khai trên nhiều Switch.[2]

- Nguyên lý hoạt động của VLAN là phân chia mạng vật lý thành các phân đoạn logic, không phụ thuộc vào vị trí vật lý của thiết bị mạng. Khi dùng mạng VLAN có thể cô lập lưu lượng truy cập cho mỗi mạng logic để sử dụng tài nguyên hiệu quả hơn. Bởi vì VLAN định nghĩa các broadcast domains trong mạng lớp 2. Broadcast domains là tập hợp tất cả các thiết bị sẽ nhận được các broadcast frame có nguồn gốc từ bất kỳ thiết bị nào trong vùng. Broadcast domains thường giới hạn bởi Router vì Router không chuyển tiếp broadcast domains. Switch Layer 2 tạo ra broadcast domains dựa trên cấu hình Switch. Có thể nói Switch là cây cầu đa năng cho phép người quản trị mạng tạo ra nhiều broadcast domains. Mỗi broadcast domains giống như một cây cầu ảo riêng biệt trong một Switch. Người quản trị có thể xác định một hoặc nhiều cầu ảo (*virtual bridges*) trong một Switch. Mỗi cây cầu ảo được tạo trong switch định nghĩa một miền quảng bá mới (VLAN). Lưu lượng không thể truyền trực tiếp đến VLAN khác (*giữa broadcast domain*) trong phạm vi chuyển đổi hoặc giữa hai thiết bị chuyển mạch. Để kết nối hai Vlan khác nhau phải sử dụng Router hoặc Switch layer 3.

- Mục đích sử dụng VLAN là làm tăng băng thông cho người dùng, triển khai mạng dựa trên chức năng của người dùng và có thể thêm, bớt hoặc thay đổi vị trí các máy tính trong các mạng với nhau một cách đơn giản bởi vì Vlan dựa trên logic thay vì kết nối vật lý, chúng cực kỳ linh hoạt. Một VLAN thông thường bao gồm các cổng của một hay nhiều Switch cùng nằm trong cùng broadcast domain. Các cổng có thể được đưa vào các VLAN khác nhau trên một hay nhiều Switch bằng cách tạo ra nhiều VLAN, các Switch sẽ tạo ra nhiều broadcast domain. Khi đó một broadcast domain là một VLAN, và thông tin quảng bá sẽ không được chuyển tiếp đến các máy tính trong VLAN khác.

- Khi nào sử dụng VLAN: Tăng cường việc quản lý bảo mật; Quá nhiều thiết bị trong một mạng gây hiện tượng quá tải; Một nhóm làm việc thường xuyên có nhu cầu trao đổi một lượng thông tin lớn qua mạng làm ảnh hưởng đến băng thông của phần còn lại, hay một nhóm sử dụng

chung một loại dịch vụ nào đó, khi đó nên nhóm vào một VLAN; Tiết kiệm thiết bị cho hệ thống.

- Dãy giá trị VLAN-ID chạy từ 0 – 4095: [1]

+ Dải từ 1 đến 1001: VLAN thường được sử dụng.

+ Dải từ 1002 đến 1005: thường dùng để giao tiếp với các kiểu mạng LAN khác.

+ Dải từ 1006 đến 4094: VLAN mở rộng, sử dụng khi switch hoạt động ở mode Transparent.

+ 0 và 4095: VLAN dành riêng.

+ VLAN 1, 1002 – 1005: mặc định trên Switch và không thể xóa được.

Mặc định VLAN sau khi được tạo sẽ được lưu vào file vlan.dat trong bộ nhớ Flash.

- Các loại VLAN (*5 loại VLAN thường được sử dụng*):

+ VLAN 1: Đây là kiểu mạng mặc định của tất tất cả các thiết bị Switch hỗ trợ VLAN và nó hoạt động ở Lớp 2 (*Data Link layer*), vì vậy nếu hệ thống mạng máy tính được trang bị thiết bị Switch có hỗ trợ chức năng này mà chúng ta chưa cấu hình các thông số kỹ thuật thì mặc định nó vẫn có thể chuyển tiếp các gói dữ liệu giữa các máy tính và thiết bị kết nối vào nó một cách bình thường như các thiết bị chuyển mạch khác, vì tất cả các cổng mạng trên Switch mặc định đều nằm trong cùng một miền quảng bá và với sự quản lý của VLAN 1.

+ Default VLAN: Là kiểu VLAN mặc định ban đầu với tất cả các cổng giao tiếp trên thiết bị chuyển mạch, vì vậy Default VLAN cũng có thể hiểu là VLAN 1, và các VLAN khác như User VLAN, Native VLAN, Management VLAN đều là các thành phần con của Default VLAN.

+ User VLAN: Là VLAN trong đó chứa các tài khoản người dùng thành từng nhóm dựa theo các thuộc tính về đặc thù công việc của từng nhóm làm việc hay theo thuộc tính về vị trí vật lý của các nhóm làm việc này.

+ Native VLAN: Là VLAN dùng để cấu hình Trunking do một số thiết bị không tương thích với nhau, lúc này ta phải sử dụng Native VLAN để chúng có thể giao tiếp với nhau. Khi đó, tất cả các khung dữ liệu (frame) của các VLAN khi giao tiếp qua kết nối Trunking đều sẽ được gắn Tag của giao thức 802.1Q hoặc ISL, ngoại trừ các frame của VLAN 1. Native VLAN là VLAN mà frame của nó sẽ không được Tag trước khi gửi qua đường Trunk. Ngầm định Native VLAN của Switch là VLAN 1.

+ Management VLAN: Để có thể giám sát từ xa các thiết bị Switch trong hệ thống mạng chúng ta cần phải có một VLAN đặc biệt dùng để thực hiện việc này, đó chính là Management VLAN. Bằng cách gán một địa chỉ IP dùng để Telnet từ xa vào hệ thống mạng thông qua địa chỉ IP này, và có thể cấm người dùng khác truy cập vào thiết bị. Vì đây là một VLAN đặc biệt được cấp một số quyền quản trị nên nó cần phải được tách riêng ra khỏi các VLAN khác để đảm bảo yếu tố an toàn bảo mật. Khi mạng có vấn đề như: hội tụ với STP, broadcast storms thì một Management VLAN cho phép nhà quản trị vẫn có thể truy cập được vào thiết bị và giải quyết vấn đề đó.

+ Voice VLAN: Là VLAN dành cho lưu lượng thoại. Nó cho phép các cổng Switch mang lưu lượng thoại IP từ một điện thoại IP. Người quản trị mạng cấu hình một Voice VLAN và gán nó để truy cập các cổng. Khi một điện thoại IP được kết nối với các cổng Switch, Switch sẽ gửi gói tin CDP đó hướng dẫn các điện thoại IP đính kèm để gửi lưu lượng thoại được gán nhãn VLAN ID.

- Các kiểu VLAN (*có 3 kiểu VLAN phổ biến*): [1]

Port - based VLAN (*VLAN dựa trên cổng*): Đây là cách cấu hình VLAN đơn giản và phổ biến nhất. Cấu hình này cho phép người quản trị mạng gắn VLAN theo cách thủ công, mỗi cổng Switch được gắn vào một VLAN xác định. Port - based VLAN thích hợp với hệ thống mạng có quy mô nhỏ và không phải thường xuyên thay đổi hạ tầng.

MAC address based VLAN (*VLAN dựa trên địa chỉ MAC*): đề cập đến việc gắn các VLAN theo địa chỉ MAC - mỗi địa chỉ MAC được đánh dấu với một VLAN. Cách cấu hình này không được sử dụng nhiều do còn nhiều hạn chế trong việc quản lý.

Protocol - based VLAN (*VLAN dựa trên giao thức*): cách cấu hình này tương tự như MAC

address based VLAN, nhưng chỉ dùng duy nhất một địa chỉ IP hoặc địa chỉ logic thay thế cho địa chỉ MAC. Hiện nay, cách cấu hình này đã không còn quá thông dụng nhờ sử dụng giao thức DHCP.

- Các bước chia VLAN

Để chia VLAN chúng ta thường dựa vào cấu hình của các thiết bị mạng như Switch hoặc Router, sau đây là các bước cơ bản để thực hiện chia VLAN:

Bước 1: Xác định các nhóm thiết bị. Đầu tiên, chúng ta cần xác định các nhóm máy tính, thiết bị hoặc người dùng muốn tách biệt vào các VLAN khác nhau. Điều này có thể dựa trên phòng ban, chức năng công việc, hoặc các yếu tố tương tự.

Bước 2: Cấu hình Switch. Trong môi trường mạng, switch đóng một vai trò quan trọng trong việc tạo và quản lý các VLAN. Chúng ta cần cấu hình switch để gán các cổng (port) vào từng VLAN cụ thể. Mỗi cổng có thể thuộc một hoặc nhiều VLAN tùy theo yêu cầu.

Bước 3: Cấu hình Router (nếu cần). Nếu chúng ta muốn tạo kết nối giữa các VLAN khác nhau hoặc kết nối ra ngoài mạng, chúng ta cần một Router. Router sẽ giúp định tuyến dữ liệu giữa các VLAN và gói tin có thể được chuyển giữa các mạng con.

Bước 4: Cấu hình bảo mật và quy tắc truy cập. Một trong những lợi ích quan trọng của VLAN là khả năng áp dụng quy tắc bảo mật tùy chỉnh cho từng VLAN. Chúng ta có thể cấu hình các quy tắc truy cập để quản lý việc trao đổi dữ liệu giữa các VLAN và kiểm soát truy cập không mong muốn.

- Sau đây là bảng so sánh một số tiêu chí cơ bản giữa LAN và VLAN trong mạng máy tính:

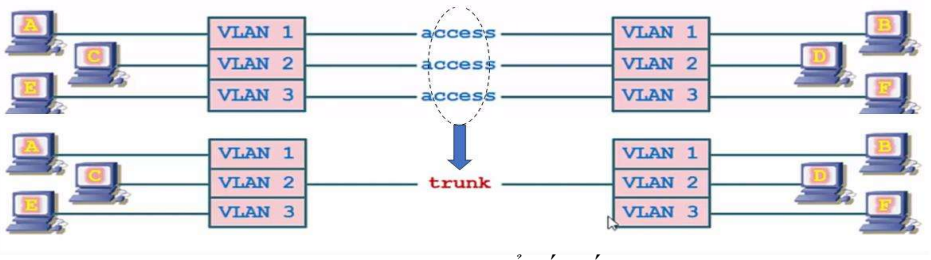
Tiêu chí	LAN	VLAN
Khái niệm	Mạng nội bộ kết nối các thiết bị trong một khu vực giới hạn.	Mạng logic được tạo ra trên cơ sở mạng vật lý hiện có.
Phạm vi kết nối	Giới hạn trong một khu vực vật lý như tòa nhà hoặc khuôn viên.	Có thể kết nối các thiết bị nằm ở nhiều vị trí địa lý khác nhau.
Phân đoạn mạng	Tất cả các thiết bị trong một LAN chia sẻ cùng một broadcast domain.	VLAN chia broadcast domain thành các phần nhỏ hơn, mỗi VLAN là một broadcast domain riêng.
Quản lý tài nguyên	Tất cả các thiết bị dùng chung một tập hợp tài nguyên mạng.	VLAN cho phép phân bổ tài nguyên mạng theo nhóm người dùng hoặc chức năng.
Độ phức tạp	Đơn giản trong triển khai và quản lý.	Phức tạp hơn do yêu cầu cấu hình và quản lý từng VLAN.
Bảo mật	Bảo mật kém vì không có cơ chế phân tách mạng logic.	Tăng cường bảo mật thông qua phân tách và kiểm soát truy cập từng VLAN.
Chi phí	Thấp hơn do không cần thiết bị hỗ trợ đặc biệt.	Chi phí cao hơn do yêu cầu thiết bị hỗ trợ VLAN và công tác cấu hình.
Ứng dụng	Thường sử dụng trong các văn phòng nhỏ hoặc gia đình.	Thường được áp dụng trong các doanh nghiệp lớn và trung tâm dữ liệu.
Hiệu suất	Có thể giảm hiệu suất khi mạng mở rộng và lưu lượng broadcast tăng.	Hiệu suất cao hơn nhờ giới hạn broadcast trong từng VLAN.
Thay đổi và mở rộng	Mở rộng bằng cách thêm thiết bị và dây cáp mạng.	Dễ dàng mở rộng và thay đổi cấu trúc logic mạng mà không cần thay đổi cấu trúc vật lý.

2.2. Kỹ thuật TRUNK

Trunk là một kỹ thuật truyền tải dữ liệu giữa các Vlan khác nhau thông qua một kết nối vật lý duy nhất. Khi mạng có nhiều Vlan để phân chia và quản lý thì cần có TRUNK để chuyển dữ liệu giữa chúng một cách hiệu quả. Kết nối TRUNK là liên kết Point - to - Point giữa các cổng trên Switch với Router hoặc với Switch khác. Kết nối TRUNK sẽ truyền tải dữ liệu của nhiều

Vlan thông qua một liên kết đơn và cho phép mở rộng Vlan trên hệ thống mạng. Vì kỹ thuật này cho phép dùng chung một kết nối vật lý cho dữ liệu của các Vlan đi qua nên để phân biệt được chúng là dữ liệu của Vlan nào, khi đó người ta gắn vào các gói tin một thẻ gọi là "*tagging*" hay nói một cách khác là dùng một kiểu đóng gói riêng cho các gói tin di chuyển qua đường TRUNK, đường TRUNK này phải chạy giao thức đường truyền đặc biệt đó là giao thức độc quyền ISL của Cisco hoặc IEEE chuẩn 802.1Q (dot1q). [2]

Ví dụ: Trường ĐH Hoa Lư có 3 phòng chức năng được đặt tên là: VN1, VN2, VN3, cả 3 phòng chức năng này đều được đặt ở 2 toà nhà khác nhau. Người quản trị mạng đặt tên Vlan cho 3 phòng chức năng lần lượt là: Vlan 1, Vlan 2, Vlan 3 để thuận tiện cho quá trình làm việc và quản lý. Thay vì phải dùng 3 đường dây mạng để kết nối giữa 3 Vlan ở 2 toà nhà, người quản trị mạng đã sử dụng kỹ thuật TRUNK để kết nối, tức là sử dụng 1 đường dây mạng duy nhất để kết nối dữ liệu giữa 3 Vlan của 2 toà nhà.



Hình 1: Sử dụng Trunk để kết nối các Vlan

Trên Switch có 2 loại cổng chính, mỗi cổng phụ trách nhiệm vụ riêng:

+ Access Port (*cổng truy cập*): Các cổng truy cập được cấu hình để thuộc về một Vlan cụ thể. Các thiết bị được kết nối vào cổng truy cập này sẽ trở thành thành viên của Vlan đó. Các cổng truy cập không gắn thẻ (*untagged*), nghĩa là khi dữ liệu ra khỏi cổng, nó không được gắn thêm thông tin về Vlan.

+ Trunk Port (*cổng Trunk hoặc cổng trung kế*) Các cổng TRUNK được cấu hình để có khả năng chuyển dữ liệu của nhiều Vlan khác nhau qua một kết nối vật lý. Cổng TRUNK gắn thẻ (*tagged*) dữ liệu với các thẻ Vlan để cho phép các thiết bị khác biết dữ liệu thuộc về Vlan nào. Điều này cho phép truyền tải dữ liệu giữa các Vlan qua cùng một cổng vật lý.

2.3. Giao thức DHCP

DHCP (*Dynamic Host Configuration Protocol*) là một giao thức mạng được sử dụng để tự động cấp phát các địa chỉ IP và cấu hình liên quan khác cho các thiết bị trong mạng. Giao thức này cho phép các thiết bị kết nối vào mạng một cách linh hoạt và tiện lợi, giúp giảm thiểu sự can thiệp thủ công và giúp tối ưu hóa việc quản lý mạng. [3]

Khi một thiết bị muốn tham gia vào mạng, nó gửi yêu cầu DHCP đến máy chủ DHCP trong mạng khi đó máy chủ DHCP sẽ đáp ứng yêu cầu này và cung cấp một địa chỉ IP duy nhất, Subnet mask (*mặt nạ con*), Default gateway (*cổng mặc định*), DNS servers (*máy chủ DNS*) và các thông tin cấu hình mạng khác cho thiết bị đó. Quá trình này diễn ra tự động và nhanh chóng, giúp thiết bị nhanh chóng kết nối và hoạt động trong mạng. Giao thức DHCP giúp tránh xung đột địa chỉ IP, tiết kiệm thời gian và công sức trong việc cấu hình mạng thủ công, và hỗ trợ quản lý mạng hiệu quả hơn. Với DHCP, việc thêm hoặc thay đổi các thiết bị trong mạng trở nên dễ dàng và linh hoạt hơn, đồng thời giúp duy trì tính sắp xếp và tổ chức của mạng một cách hiệu quả. Hiện nay giao thức DHCP có 2 version cho IPv4 và IPv6. Cấu hình địa chỉ IP sẽ được người quản trị mạng thiết lập trên DHCP server.

- Các gói tin chính của DHCP Server:

+ Gói tin Discover: Một DHCP Client khi mới tham gia vào hệ thống mạng. Nó sẽ yêu cầu thông tin địa chỉ IP từ DHCP Server bằng cách gửi bản tin broadcast một gói DHCP Discover có địa chỉ nguồn là 0.0.0.0 để tìm kiếm DHCP Server vì client chưa có địa chỉ IP.

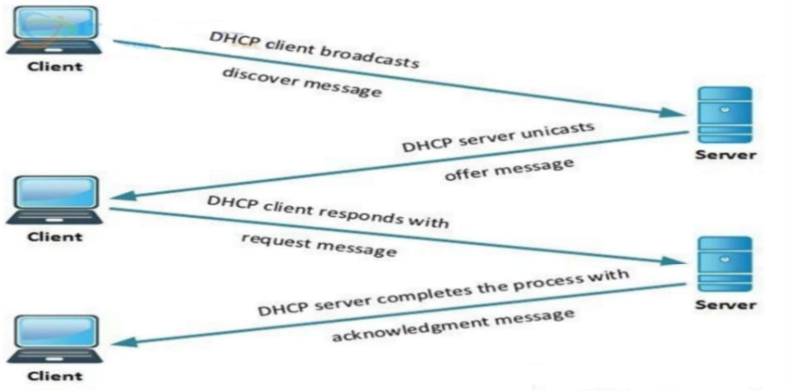
+ Bản tin Offer: Khi DHCP Server nhận được gói DHCP Discover từ client. Nó sẽ gửi lại một gói DHCP Offer chứa các thông số như địa chỉ IP, Subnet Mask, Gateway,…cho client Có

thể nhiều DHCP server sẽ gửi lại gói DHCP Offer nhưng Client chỉ chấp nhận gói DHCP Offer đầu tiên nó nhận được.

+ DHCP Request Packet: Khi DHCP Client nhận được một gói DHCP Offer. Nó đáp lại bằng việc gửi bản tin DHCP Request để xác nhận hoặc kiểm tra lại các thông tin mà DHCP Server vừa gửi.

+ DHCP Acknowledge: Server kiểm tra và xác nhận lại sự chấp nhận thuê địa chỉ IP từ client.

- Các bước DHCP hoạt động:



Hình 2: Sơ đồ hoạt động của DHCP

Bước 1: Yêu cầu (*Discover*) Khi một thiết bị muốn kết nối vào mạng (*client*), nó gửi một yêu cầu DHCP broadcast (*gửi đến tất cả các thiết bị trong mạng và có chứa địa chỉ MAC của client*) để tìm kiếm máy chủ DHCP Server để nhận các thông tin cấu hình mạng.

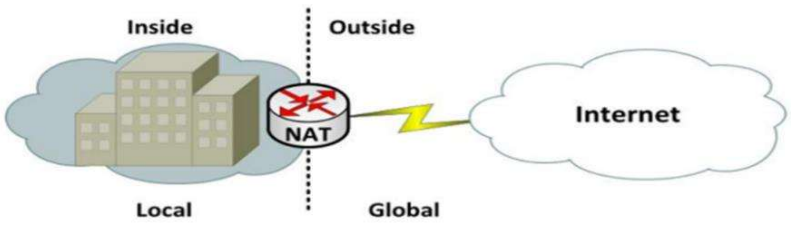
Bước 2: Cung cấp (*Offer*) Các máy chủ DHCP Server trong mạng nhận được yêu cầu và đáp ứng bằng cách gửi một gói tin chứa thông tin cấu hình DHCP. Gói tin này gọi là "Offer" và chứa một địa chỉ IP khả dụng mà DHCP Server đề xuất cho client. Nếu có nhiều máy chủ DHCP thì client sẽ nhận được nhiều gói "Offer" và chọn một gói "Offer" duy nhất để tiếp tục quá trình.

Bước 3: Chấp nhận (*Request*) Client nhận được gói "Offer" từ máy chủ DHCP Server và chọn một địa chỉ IP trong gói "Offer" hoặc gửi yêu cầu tiếp theo tới máy chủ DHCP xác nhận việc sử dụng địa chỉ IP đó. Yêu cầu này gọi là "*Request.*"

Bước 4: Xác nhận (*Acknowledge*) Máy chủ DHCP Server nhận được yêu cầu "*Request*" từ client và xác nhận rằng địa chỉ IP đã được gán cho thiết bị. Nó gửi một gói "*Acknowledge*" chứa các thông tin cấu hình mạng đã được chấp nhận và cho phép thiết bị sử dụng địa chỉ IP và cấu hình này.

2.4. Kỹ thuật NAT

NAT (*Network Address Translation*) là một kỹ thuật kết nối mạng được sử dụng để chuyển đổi địa chỉ IP giữa những mạng khác nhau. Khi một thiết bị trong mạng LAN muốn truy cập ra ngoài Internet, NAT sẽ thực hiện chuyển đổi địa chỉ IP của thiết bị trong mạng LAN (*IP Private*) sang địa chỉ IP công cộng (*IP Public*) để có thể kết nối với Internet. NAT giúp giảm thiểu số lượng địa chỉ IP Public cần sử dụng và cũng giúp bảo vệ mạng riêng khỏi các cuộc tấn công từ bên ngoài. [2]



Hình 3: Mô hình mạng sử dụng kỹ thuật NAT

- Giải thích các loại địa chỉ trong Hình 3:

+ Địa chỉ inside local: là địa chỉ IP gán cho một thiết bị mạng bên trong, địa chỉ này hầu như không phải địa chỉ được cấp bởi NIC hay nhà cung cấp dịch vụ.

+ Địa chỉ inside global: là địa chỉ đã được đăng ký với NIC, dùng để thay thế một hay nhiều địa chỉ IP inside local.

+ Địa chỉ outside local: là địa chỉ IP của một thiết bị bên ngoài khi nó xuất hiện bên trong mạng, địa chỉ này không nhất thiết là địa chỉ được đăng ký, nó được lấy từ không gian địa chỉ bên trong.

+ Địa chỉ outside global: là địa chỉ IP gán cho một thiết bị mạng bên ngoài, địa chỉ này được lấy từ địa chỉ có thể dùng để định tuyến toàn cầu hay từ không gian địa chỉ mạng.

- Ba kỹ thuật NAT thường được sử dụng là:

+ Static NAT được sử dụng để ánh xạ địa chỉ theo kiểu "*one - to - one*" và được chỉ định bởi người quản trị mạng.

+ Dynamic NAT là kiểu chuyển dịch địa chỉ dạng "*one - to - one*" một cách tự động.

+ NAT Overload là kiểu chuyển dịch địa chỉ dạng "*many - to - one*" một cách tự động, sử dụng các chỉ số cổng (port) để phân biệt cho từng dịch chuyển.

- Chức năng của NAT:

+ Chuyển đổi địa chỉ IP: NAT thực hiện chuyển đổi địa chỉ IP của các thiết bị trong mạng nội bộ thành địa chỉ IP của một thiết bị bên ngoài, giúp các thiết bị trong mạng nội bộ có thể truy cập được Internet.

+ Bảo vệ mạng: NAT giúp bảo vệ mạng nội bộ khỏi các cuộc tấn công từ mạng bên ngoài bằng cách giấu địa chỉ IP thực của các thiết bị trong mạng.

+ Quản lý kết nối: NAT theo dõi các kết nối mạng và duy trì bảng NAT để đảm bảo rằng các gói tin được gửi đến đúng thiết bị trong mạng nội bộ.

+ Tiết kiệm địa chỉ IP: NAT giúp tiết kiệm địa chỉ IP bằng cách sử dụng một địa chỉ IP công cộng (*IP Public*) duy nhất để đại diện cho toàn bộ thiết bị trong mạng nội bộ.

2.5. Sơ lược phần mềm giả lập EVE-NG

Hiện nay có rất nhiều phần mềm giả lập mạng nhưng hiện tại có ba phần mềm phổ biến đó là Cisco Packet Tracer, GNS3 và EVE-NG. Nhờ đó việc mô phỏng các thiết bị mạng để học tập, thiết kế và nghiên cứu network sẽ đơn giản đi rất nhiều.

Trong đó EVE-NG có nhiều ưu điểm vượt trội so với các phần mềm giả lập khác đó là: EVE-NG là một nền tảng mã nguồn mở cho phép người dùng thiết kế các mạng từ đơn giản đến phức tạp bằng giao diện dựa trên Web. EVE-NG hỗ trợ một loạt công nghệ ảo hóa như VMware, KVM và VirtualBox, đồng thời cho phép người dùng chạy hình ảnh NOS từ nhiều nhà cung cấp khác nhau. Một số tính năng chính của EVE-NG là: Hỗ trợ hình ảnh NOS của nhiều nhà cung cấp; giao diện dựa trên web để dễ sử dụng; tích hợp với các nền tảng đám mây như AWS và GCP; tự động hóa mạng và khả năng lập trình thông qua tập lệnh Python; hỗ trợ các chức năng mạng ảo hóa (VNF).

Ưu điểm: Hỗ trợ nhiều loại thiết bị và phần mềm mạng; cung cấp công nghệ ảo hóa và đám mây tiên tiến; cung cấp giao diện dựa trên web để dễ dàng truy cập và quản lý; cho phép người dùng chạy hình ảnh thiết bị trong thế giới thực.

2.6. Ứng dụng cấu hình Lab trên phần mềm giả lập EVE-NG

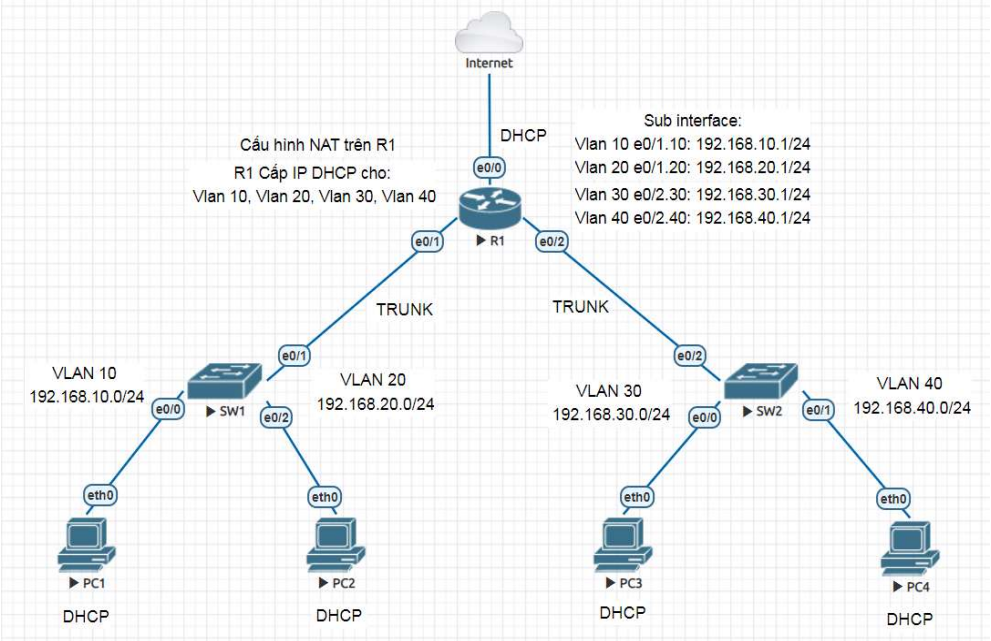
- Sơ đồ bài Lab được thiết kế trên phần mềm giả lập Eve-Ng.

- Yêu cầu bài Lab:

+ Thiết bị: 1 Router Cisco; 2 Switch Cisco; 4 PC; 1đường internet; Cáp Fast Ethernet.

+ Cấu hình trên Switch: Cấu hình trên các Interface; chia VLAN và gắn Port trên Switch; cấu hình Trunk; kiểm tra kết nối giữa các thiết bị trong mạng.

+ Cấu hình trên Router: Cấu hình các sub-Interface trên Router R1 tương ứng với các VLANs; cấu hình DHCP; cấu hình NAT Overload.



Hình 4. Sơ đồ mạng logic

- Mục tiêu bài Lab:

+ Cấu hình VLAN 10, VLAN 20, VLAN 30, VLAN 40, TRUNK, DHCP trên SW1, SW2 và R1 để PC1, PC2, PC3, PC4 nhận được IP động; các PC1, PC2, PC3, PC4 Ping thông được với nhau (*hình 4*).

+ Cấu hình NAT Overload địa chỉ của các máy tính trong mạng nội bộ ra được ngoài Internet

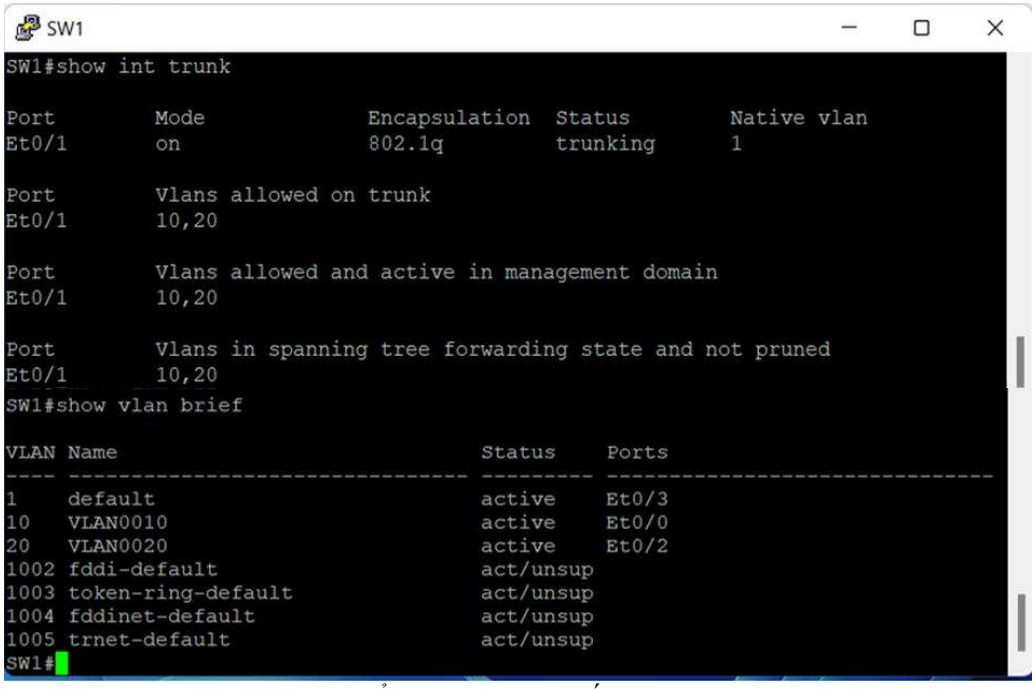
+ Đạt được: Ping 8.8.8.8 thành công; Ping http://hluv.edu.vn thành công.

- Code cấu hình trên các thiết bị:

+ Cấu hình trên SW1

```
hostname SW1
vlan 10
vlan 20
exit
int e0/0
switchport mode access
switchport access vlan 10
exit
int e0/2
switchport mode access
switchport access vlan 20
exit
int e0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20
exit
```

Sau khi cấu hình trên SW1 chúng ta thực hiện kiểm tra thông tin đường Trunk, Native-vlan và kiểm tra thông tin Vlan tương ứng với các access-port bằng các câu lệnh "*show int trunk*" và "*show vlan brief*" (*hình 5*), quá trình này cung cấp một cái nhìn tổng quan và chi tiết về trạng thái của các kết nối Trunk, và các Vlan trên switch. Đồng thời những thông tin thu được này là cơ sở để đánh giá và điều chỉnh cấu hình mạng để đảm bảo tính ổn định và hiệu quả của hệ thống mạng.

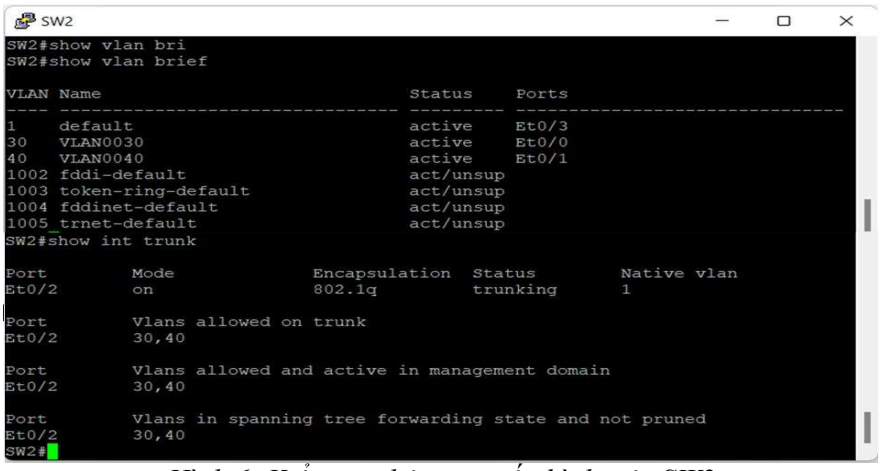


Hình 5: Kiểm tra thông tin cấu hình trên SW1

Câu lệnh "*show int trunk*" cung cấp thông tin chi tiết về các kết nối Trunk trên Switch, trong hình 5 chúng ta thấy cổng e0/1 trên SW1 đang hoạt động trong chế độ Trunk, sử dụng chuẩn 802.1q có native vlan là 1 và các VLAN 10, 20 được phép thông qua các kết nối này. Kết quả từ câu lệnh này giúp người quản trị mạng đảm bảo rằng các kết nối Trunk được cấu hình đúng cách và các VLAN được chuyển tiếp một cách chính xác giữa các switch trong mạng.

Câu lệnh "*show vlan brief*" hiển thị danh sách các VLAN 10, VLAN 20 hiện có trên switch cùng với các thông tin quan trọng như VLAN ID, tên VLAN và trạng thái của chúng. Kết quả từ câu lệnh này cho thấy việc phân chia VLAN đã được thực hiện đúng cách, cũng như xác định các VLAN đang hoạt động và có trạng thái ổn định.

+ Cấu hình trên SW2hostname SW2
vlan 30
vlan 40
exit
int e0/0
switchport mode access
switchport access vlan 30
exit
int e0/1
switchport mode access
switchport access vlan 40
exit
int e0/2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 30,40
exit



Hình 6: Kiểm tra thông tin cấu hình trên SW2

Câu lệnh "*show vlan brief*" (*hình 6*) hiển thị danh sách các VLAN 30, VLAN 40 hiện có trên switch cùng với các thông tin quan trọng như VLAN ID, tên VLAN và trạng thái của chúng. Kết quả từ câu lệnh này cho thấy việc phân chia VLAN đã được thực hiện đúng cách, cũng như xác định các VLAN đang hoạt động và có trạng thái ổn định.

Câu lệnh "*show int trunk*" cung cấp thông tin chi tiết về các kết nối Trunk trên Switch, trong hình trên chúng ta thấy cổng e0/2 trên SW2 đang hoạt động trong chế độ Trunk, sử dụng chuẩn 802.1q có native vlan là 1 và các VLAN 30, 40 được phép thông qua các kết nối này. Kết quả từ câu lệnh này giúp người quản trị mạng đảm bảo rằng các kết nối Trunk được cấu hình đúng cách và các VLAN được chuyển tiếp một cách chính xác giữa các switch trong mạng.

+ Code cấu hình trên R1

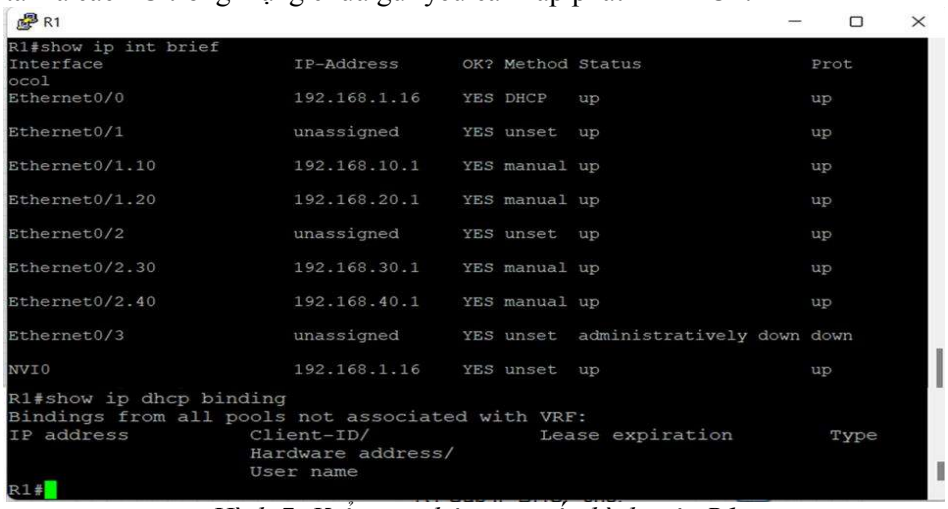
```
hostname R1
int e0/0
no shut
ip address dhcp
exit
// Code cấu hình Sub interface trên cổng e0/1 cho Vlan 10, Vlan 20
int e0/1
no shut
exit
int e0/1.10
encapsulation dot1q 10
ip address 192.168.10.1 255.255.255.0
no shut
exit
int e0/1.20
encapsulation dot1q 20
ip address 192.168.20.1 255.255.255.0
no shut
exit
// Code cấu hình Sub interface trên cổng e0/2 cho Vlan 30, Vlan 40
int e0/2
no shut
exit
int e0/2.30
encapsulation dot1q 30
ip address 192.168.30.1 255.255.255.0
```

```
no shut
exit
int e0/2.40
encapsulation dot1q 40
ip address 192.168.40.1 255.255.255.0
no shut
exit
//Code cấu hình DHCP cho Vlan 10, Vlan 20, Vlan 30, Vlan 40
ip dhcp pool VLAN10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 8.8.8.8
ip dhcp excluded-address 192.168.10.1 192.168.10.20
ip dhcp pool VLAN20
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
dns-server 8.8.8.8
ip dhcp excluded-address 192.168.20.1 192.168.20.20
ip dhcp pool VLAN30
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
dns-server 8.8.8.8
ip dhcp excluded-address 192.168.30.1 192.168.30.20
ip dhcp pool VLAN40
network 192.168.40.0 255.255.255.0
default-router 192.168.40.1
dns-server 8.8.8.8
ip dhcp excluded-address 192.168.40.1 192.168.40.20
// Code cấu hình NAT
access-list 1 permit any
ip nat inside source list 1 interface e0/0 overload
int e0/0
ip nat outside
exit
int e0/1.10
ip nat inside
exit
int e0/1.20
ip nat inside
exit
int e0/2.30
ip nat inside
exit
int e0/2.40
ip nat inside
exit
```

Để kiểm tra và xác nhận thông tin cấu hình trên router (R1) chúng ta sử dụng câu lệnh "*show ip int brief*" và "*show ip dhcp binding*" *(hình 7*). Các câu lệnh này cung cấp thông tin chi tiết và tổng quan về cấu hình mạng trên router, từ đó giúp chúng ta hiểu rõ hơn về trạng thái của router và cách quản lý các địa chỉ IP được cấp phát trong mạng.

Câu lệnh "*show ip int brief*" cho chúng ta biết các thông tin về các giao diện (*interface*), địa chỉ IP address, trạng thái của mỗi giao diện (*method status*) của R1 đã được cấu hình chính xác và có trạng thái đang hoạt động ổn định.

Câu lệnh "*show ip dhcp binding*" cung cấp bảng thông tin về các thiết bị kết nối vào mạng thông qua dịch vụ DHCP trên router R1. Lúc này bảng thông tin về địa chỉ IP trong *hình 7* chưa có bởi vì tất cả các PC trong mạng chưa gửi yêu cầu cấp phát IP DHCP.



Hình 7: Kiểm tra thông tin cấu hình trên R1

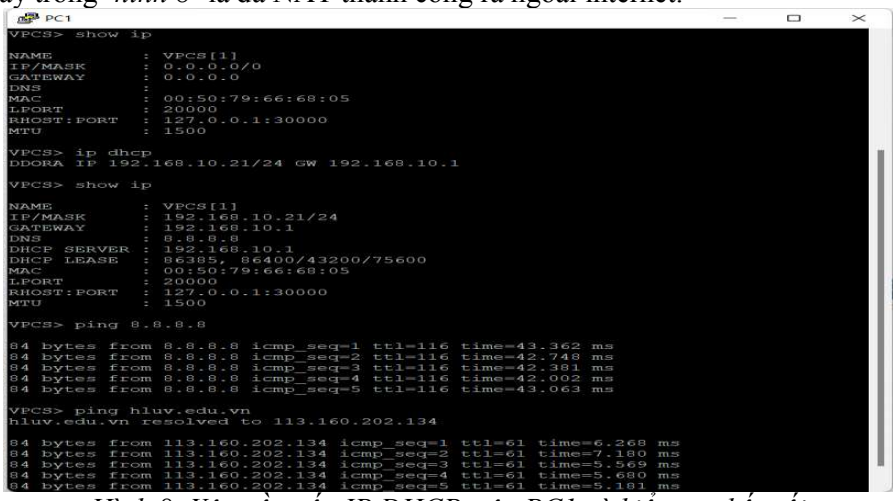
Kiểm tra cấp phát địa chỉ Ip và kiểm tra sự kết nối mạng giữa các Vlan và kết nối ra internet.

+Trên PC1:

Ban đầu khi thực hiện lệnh "*show ip*" thì PC1 chưa có bất cứ thông tin nào về IP.

Tiếp theo chúng ta thực hiện lệnh "*ip dhcp*" thì PC1 nhận được đầy đủ thông tin về địa chỉ IP, subnet mask, Gategay, DNS,… từ dịch vụ DHCP (*hình 8*).

Sau khi xác nhận thông tin IP, bước tiếp theo là kiểm tra kết nối mạng bằng cách: từ PC1 ping tới một địa chỉ IP bên ngoài internet "*ping 8.8.8.8*" một địa chỉ IP của máy chủ DNS của Google; "*ping hluv.edu.vn*" một địa chỉ máy chủ của trường Đại học Hoa Lư và kết quả như chúng ta thấy trong '*hình 8*' là đã NAT thành công ra ngoài internet.

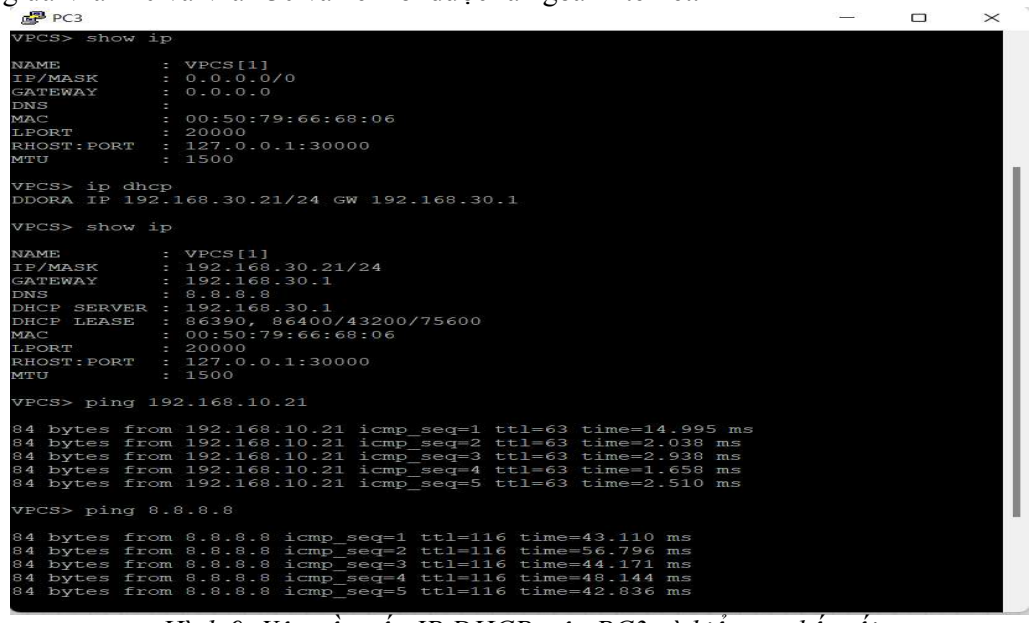


Hình 8: Yêu cầu cấp IP DHCP trên PC1 và kiểm tra kết nối

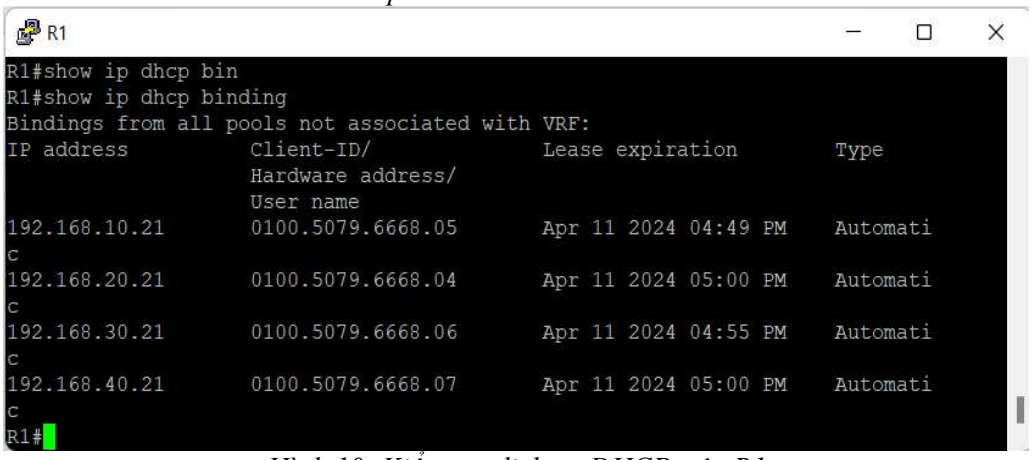
+ Trên PC 3:

Tương tự như PC1, ban đầu khi thực hiện lệnh "*show ip*" thì PC3 chưa có bất cứ thông tin nào về IP. Sau đó thực hiện lệnh "*ip dhcp*" thì PC3 nhận được đầy đủ thông tin về địa chỉ IP, subnet mask, Gategay, DNS,… từ dịch vụ DHCP (*hình 9*).

Sau khi xác nhận thông tin IP, bước tiếp theo là kiểm tra kết nối giữa các Vlan trong mạng bằng cách từ PC3 ping tới địa chỉ IP của PC1 thuộc Vlan 10 "ping 192.168.10.21"; kiểm tra kết nối ra ngoài internet: "*ping 8.8.8.8*" và kết quả như chúng ta thấy trong '*hình 9*' đã ping thành công giữa Vlan 10 và Vlan 30 và kết nối được ra ngoài internet.



Hình 9: Yêu cầu cấp IP DHCP trên PC3 và kiểm tra kết nối



Hình 10: Kiểm tra dịch vụ DHCP trên R1

Sau khi các PC1, PC2, PC3, PC4 đã được cấp địa chỉ IP từ dịch vụ DHCP thành công, tại router R1 chúng ta thực hiện lệnh "*show ip dhcp binding*" thì lúc này xuất hiện bảng thông tin địa chỉ IP của các PC kết nối vào mạng thông qua dịch vụ DHCP (*hình 10*). Điều này giúp chúng ta theo dõi và quản lý các thiết bị kết nối vào mạng một cách hiệu quả.

3. Kết luận

Quá trình nghiên cứu lý thuyết và ứng dụng thực hành bài Lab trên phần mềm giả lập EVE-NG, tác giả đã đạt được những kết quả đáng kể trong việc hiểu và áp dụng các khái niệm này vào thực tế cụ thể như: Đã nắm vững cách cấu hình và quản lý Vlan, nhận thức rõ vai trò của VLAN trong việc chia mạng vật lý thành nhiều mạng logic để tăng cường bảo mật và hiệu suất mạng; hiểu rõ cách thiết lập và quản lý kết nối Trunk, đảm bảo truyền thông hiệu quả giữa các VLAN trên các thiết bị mạng; thành thạo trong việc cấu hình và quản lý dịch vụ DHCP, tự động cấp phát địa chỉ IP và thông tin cấu hình mạng cho các thiết bị; nắm bắt kỹ thuật cấu hình và quản lý NAT. Những kiến thức này không chỉ mang lại cái nhìn tổng quan và sâu sắc về công nghệ mạng mà còn tạo nền tảng vững chắc cho việc tiếp tục nghiên cứu và phát triển trong lĩnh

vực thiết kế, cấu hình và quản lý mạng máy tính. Hướng phát triển tiếp theo sẽ tập trung vào ứng dụng những hiểu biết này vào các tình huống mạng phức tạp hơn và khám phá thêm các công nghệ mạng tiên tiến khác.

TÀI LIỆU THAM KHẢO

[1] Cisco networking academy (2021), *CCNA: Enterprise Networking, Security, and Automation*, https://lms.netacad.com/course/view.php?id=2149158.

[2] Huỳnh Nguyên Chính (2013), *Giáo trình mạng máy tính nâng cao*, NXB Đại học Quốc Gia TP. Hồ Chí Minh.

[3] Khương Anh, Nguyễn Hồng Sơn (2005), *Giáo trình hệ thống mạng máy tính CCNA*, NXB Lao Động - Xã Hội.