

ĐẠI HỌC BÁCH KHOA HÀ NỘI  
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

# TÀI LIỆU HƯỚNG DẪN THỰC HÀNH MẠNG MÁY TÍNH IT3080

(LƯU HÀNH NỘI BỘ)

UPDATE: 22/04/2021

# MỤC LỤC

<b>1. GIỚI THIỆU.....</b>	<b>3</b>
1.1. MỤC ĐÍCH VÀ PHẠM VI CỦA TÀI LIỆU .....	3
1.2. MỤC TIÊU THỰC HÀNH .....	3
1.3. THÔNG TIN CHUNG .....	3
<b>2. CÁC QUI ĐỊNH ĐỐI VỚI SINH VIÊN .....</b>	<b>3</b>
<b>3. BÀI THỰC HÀNH SỐ 1: BẤM DÂY MẠNG .....</b>	<b>3</b>
3.1. MỤC ĐÍCH VÀ NỘI DUNG.....	3
3.2. NỘI DUNG THỰC HÀNH .....	5
<b>4. BÀI THỰC HÀNH SỐ 2: XÂY DỰNG MỘT MẠNG LAN .....</b>	<b>6</b>
4.1. MỤC ĐÍCH VÀ NỘI DUNG.....	6
4.2. NỘI DUNG THỰC HÀNH .....	8
4.3 BÁO CÁO BÀI THỰC HÀNH SỐ 2 .....	ERROR! BOOKMARK NOT DEFINED.
<b>5. BÀI THỰC HÀNH SỐ 3: ĐỊNH TUYẾN TĨNH TRONG MẠNG IP .....</b>	<b>10</b>
5.1 MỤC ĐÍCH VÀ NỘI DUNG .....	10
5.2 NỘI DUNG THỰC HÀNH .....	14
5.3. BÁO CÁO BÀI THỰC HÀNH SỐ 3 .....	14
<b>6. BÀI THỰC HÀNH SỐ 4: BÀI THỰC HÀNH SỐ 4: PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC UDP VÀ TCP.....</b>	<b>24</b>
6.1. MỤC ĐÍCH VÀ NỘI DUNG.....	24
6.2. NỘI DUNG THỰC HÀNH .....	26
<b>7. BÀI THỰC HÀNH SỐ 5: PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC DNS VÀ HTTP .....</b>	<b>34</b>
7.1. MỤC ĐÍCH VÀ NỘI DUNG.....	34
7.2. NỘI DUNG THỰC HÀNH .....	36
<b>8. PHỤ LỤC 1: LÀM QUEN VỚI CÔNG CỤ WIRESHAKR.....</b>	<b>42</b>
<b>9. PHỤ LỤC 2: PHÂN TÍCH KHUNG TIN ETHERNET.....</b>	<b>50</b>
<b>10. PHỤ LỤC 3: PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC IP VÀ ARP .....</b>	<b>60</b>
<b>11. PHỤ LỤC 4: KIỂM TRA TÌNH TRẠNG KẾT NỐI .....</b>	<b>79</b>

**12. PHỤ LỤC 5: HƯỚNG DẪN SỬ DỤNG PACKET TRACER ..... 91**

## **1. GIỚI THIỆU**

### **1.1. MỤC ĐÍCH VÀ PHẠM VI CỦA TÀI LIỆU**

### **1.2. MỤC TIÊU THỰC HÀNH**

### **1.3. THÔNG TIN CHUNG**

Thời lượng: 5 buổi, Số tiết thực hành: 3 tiết/ 1 buổi

## **2. CÁC QUI ĐỊNH ĐỐI VỚI SINH VIÊN**

1. Tuân thủ các quy định tại phòng thực hành
2. In tài liệu thực hành (bao gồm tài liệu hướng dẫn và mẫu báo cáo), đọc kỹ tài liệu và ôn tập nội dung kiến thức liên quan
3. Mang theo tài liệu thực hành khi đến thực hành
4. Làm bài thực hành theo hướng dẫn trong tài liệu. Không thực hiện các nội dung khác với hướng dẫn thực hành, trừ khi có yêu cầu của người hướng dẫn
5. Nộp báo cáo thực hành và các kết quả khác theo yêu cầu và hướng dẫn khi kết thúc buổi thực hành
6. Tất cả các bài thực hành có dấu hiệu sao chép kết quả và nội dung báo cáo dưới mọi hình thức và với bất cứ lý do nào sẽ được chấm 0 điểm.

## **3. BÀI THỰC HÀNH SỐ 1: BẤM DÂY MẠNG**

### **3.1. MỤC ĐÍCH VÀ NỘI DUNG**

#### **3.1.1. Mục đích**

Bài thí nghiệm này được thiết kế để sinh viên tạo cáp kết nối mạng.

#### **3.1.2. Thiết bị, vật tư, phần mềm cần thiết**

- Dụng cụ, vật tư bấm dây mạng:
  - Kìm bấm dây mạng
  - Đồng hồ kiểm tra cáp mạng
  - Cáp mạng TP Cat 5, đầu nối RJ45

### **3.1.2. Yêu cầu đối với sinh viên**

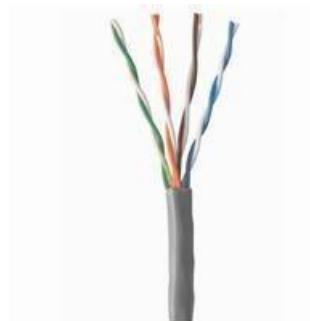
- Kiến thức:
  - Nắm vững kiến thức về chuẩn bấm cáp là T568A và T568B.
- Viết báo cáo thực hành và nộp kết quả theo yêu cầu như sau:
  - Báo cáo (bản giấy) theo mẫu đã cung cấp

### **3.1.3. Cơ sở lý thuyết**

#### **3.1.1. Mã đường truyền**

Để kết nối máy vi tính với nhau hay với các thiết bị mạng như Hub, Switch, Router,... cần phải sử dụng một loại dây cáp đặc biệt cho phép đạt tốc độ kết nối cao. Dây cáp này có thể dễ dàng mua được tại các cửa hàng vi tính hoặc các cửa hàng chuyên bán dây cáp điện, điện tử.

Đây là loại dây cáp có 8 dây nhỏ bên trong và được chia thành 4 cặp với các màu sắc khác nhau, thường được gọi là dây cáp RJ45 theo kiểu kết nối của các thiết bị mạng. Mỗi đầu dây trước khi kết nối với thiết bị mạng phải được bấm vào đầu cắm RJ45 bằng một dụng cụ chuyên dụng gọi là kềm bấm RJ45.



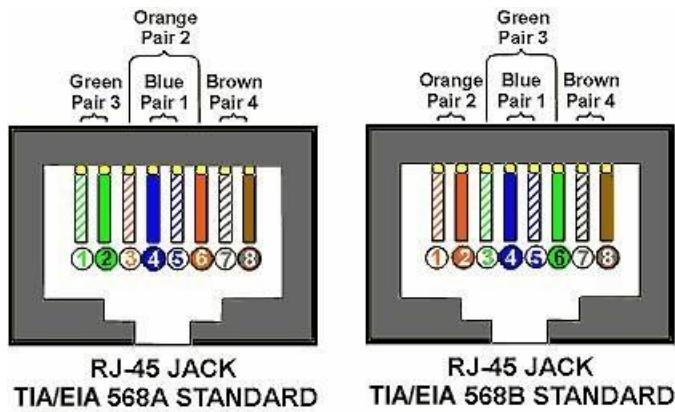
Để làm được việc này bạn cần sử dụng kìm bấm cáp mạng và hiểu được các chuẩn bấm cáp. Hiện nay có hai chuẩn bấm cáp là T568A và T568B, hai chuẩn bấm cáp này đều do Intel qui định, với các thứ tự màu như sau

**T568A:**

1. Trắng xanh lá
2. Xanh lá
3. Trắng cam
4. Xanh dương
5. Trắng xanh dương
6. Cam
7. Trắng nâu
8. Nâu

**T568B:**

1. Trắng cam
2. Cam
3. Trắng xanh lá
4. Xanh dương
5. Trắng xanh dương
6. Xanh lá
7. Trắng nâu
8. Nâu



Nếu các bạn muốn bấm một sợi dây cáp dùng để kết nối giữa các thiết bị cùng loại, ví dụ như giữa hai PC với nhau hoặc giữa hai switch (hub) với nhau, các bạn dùng kỹ thuật bấm cáp chéo (crossover cable).

Còn nếu như các bạn muốn một sợi dây cáp dùng để kết nối các thiết bị khác loại với nhau ví dụ như từ PC nối đến switch (hub) hoặc từ switch (hub) nối đến PC các bạn dùng kỹ thuật bấm cable thẳng (straight-through cable).

### **3.2. NỘI DUNG THỰC HÀNH**

#### **3.1. Tạo cáp mạng theo chuẩn T568B**

Để thực hiện đấu dây nối chéo, một đầu sợi cáp các bạn bấm chuẩn T568A và đầu còn lại các bạn bấm chuẩn T568B.

#### **3.2. Tạo cáp mạng theo chuẩn T568A**

Để thực hiện đấu dây nối thẳng, nếu một đầu sợi cáp các bạn bấm chuẩn T568A thì đầu còn lại cũng bấm chuẩn T568A, tương tự như vậy nếu một đầu bạn bấm chuẩn T568B thì đầu còn lại các bạn cũng bấm chuẩn T568B.

### **3.3. Sử dụng đồng hồ để kiểm tra dây cáp được tạo**

## **4 BÀI THỰC HÀNH SỐ 2: XÂY DỰNG MỘT MẠNG LAN**

### **4.1. MỤC ĐÍCH VÀ NỘI DUNG**

#### **4.1.1. Mục đích**

- Sinh viên xây dựng một mạng LAN đơn giản
- Quan sát và hiểu hoạt động chuyển mạch của switch trong mạng LAN

#### **4.1.2. Thiết bị, vật tư, phần mềm cần thiết**

- Switch cisco 2960c (cấu hình được)
- Switch TP link 4 FE ports
- Cáp console để cấu hình switch qua CLI
- Máy tính
- Phần mềm: bộ cài đặt cisco\_usbconsole\_driver\_3\_1.zip và terminal emulator (Putty)

#### **4.1.2. Yêu cầu đối với sinh viên**

- Môi trường thực hành:
  - Máy tính - 1 cái
- Kiến thức: Nắm vững kiến thức về giao thức ICMP, mặt nạ mạng.
- Viết báo cáo thực hành và nộp kết quả theo yêu cầu như sau:
  - Báo cáo (bản giấy) theo mẫu đã cung cấp

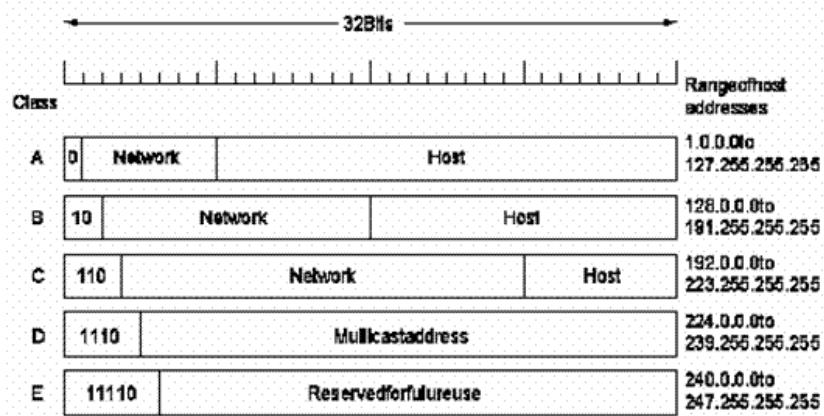
#### **4.1.3. Cơ sở lý thuyết**

Trước tiên, thiết bị switch có 4 kiểu hoạt động của giao diện điều khiển:

- USER EXEC (khi hiển thị switch> ): Kiểu này là truy cập cơ bản. Nó không cho phép truy cập vào thông tin cấu hình thiết bị.
- PRIVILEGED EXEC (khi hiển thị switch# ): Kiểu này cho phép có những thông tin cấu hình và thực hiện dò lỗi (debugging). Để chuyển lên kiểu này dùng lệnh enable. GLOBAL CONFIG (khi hiển thị switch(config)# ): Kiểu này cho phép cấu hình các tham số toàn cục. Để chuyển lên kiểu này, gõ lệnh configure terminal (hoặc gõ đơn giản là config)
- INTERFACE CONFIG (khi hiển thị switch(config-if)# ) : Kiểu này cho phép cấu hình các tham số riêng của các interfaces.

##### **4.1.3.1. Giao thức IP**

- IP (Internet Protocol) là giao thức điều khiển truyền dữ liệu trên tầng mạng trong mô hình TCP/IP. Giao thức IP chịu trách nhiệm đánh địa chỉ IP trên máy trạm, đóng gói dữ liệu nhận từ tầng giao vận vào các IP packets (gói tin IP) và vận chuyển chúng từ máy nguồn đến máy đích qua một hoặc nhiều mạng IP. Do vậy, IP định nghĩa định dạng phần tiêu đề gói tin và hệ thống đánh địa chỉ IP.
- Mỗi gói tin IP bao gồm 2 thành phần: phần tiêu đề và nội dung cần truyền. Phần tiêu đề bao gồm thông tin địa chỉ IP đích, địa chỉ IP nguồn và các thông tin cần thiết khác cho việc truyền gói tin từ nguồn đến đích. Cách thức đóng gói nội dung cần truyền, gắn tiêu đề theo từng tầng được gọi là phương thức đóng gói (encapsulation). IP hoạt động theo nguyên lý truyền thông hướng không liên kết (connectionless protocol). Cụ thể, IP không cần thiết lập liên kết giữa nơi gửi và đích nhận, ngay cả khi đích nhận này chưa từng được kết nối. Điều này có nghĩa là các gói tin IP được truyền đi mà không được đảm bảo. Chúng có thể đến đích nhận mà không còn nguyên vẹn, không theo thứ tự khi truyền.
- Giao thức IP được dùng phổ biến trên mạng Internet hiện nay với hai phiên bản chính là IPv4 và IPv6. IPv4 sử dụng 32 bit để đánh địa chỉ. Mỗi địa chỉ IPv4 được chia thành 4 số, mỗi số được lưu bởi 1 byte có giá trị từ 0 - 255. Địa chỉ IPv4 truyền thống được chia làm 5 lớp A, B, C, D, E như hình dưới đây:



- Trên thực tế, các mạng máy tính thường được chia nhỏ để phù hợp với nhu cầu sử dụng, tránh lãng phí địa chỉ IP. Các mạng nhỏ này được gọi là Subnet. Để chia nhỏ Subnet và phân biệt các mạng Subnet cần dùng một định danh gọi là Subnet Mask. Subnet mask là các số dạng 32 bit (IPv4) hoặc 128 bit (IPv6), trong đó chứa thông tin địa chỉ mạng và địa chỉ máy trạm được cung cấp. Có thể xác định địa chỉ mạng bằng cách thực hiện phép toán AND địa chỉ máy trạm bất kỳ với Subnet mask.

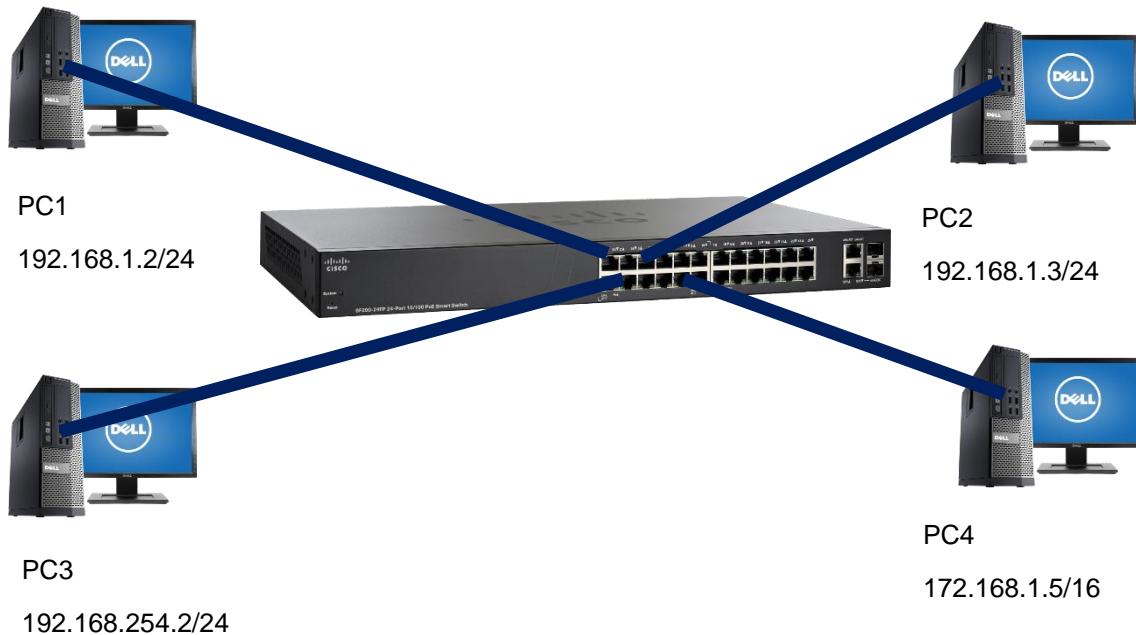
#### 4.1.3.2. Giao thức ICMP

- ICMP (Internet Control Message Protocol) là một giao thức báo cáo lỗi, thông báo cho sender biết việc gửi data đi có vấn đề, cũng giống như bộ định tuyến sử dụng để tạo thông báo lỗi đến địa chỉ IP nguồn khi các sự cố mạng ngăn chặn việc phân phôi các IP packages. ICMP tạo và gửi thư đến địa chỉ IP nguồn, cho biết rằng một gateway vào Internet mà không thể truy cập được. Mọi thiết bị mạng IP đều có khả năng gửi, nhận hoặc xử lý tin nhắn ICMP.
- ICMP không phải là giao thức truyền tải gửi dữ liệu giữa các hệ thống.
- ICMP không được sử dụng thường xuyên trong các ứng dụng người dùng cuối, nó được sử dụng bởi các quản trị mạng, nhằm mục đích khắc phục các kết nối Internet trong các tiện ích chẩn đoán (diagnostic utilities) bao gồm ping và traceroute.
- Một trong những giao thức chính của Internet Protocol suite là ICMP, ICMP được sử dụng bởi các routes, thiết bị trung gian hoặc máy chủ để truyền thông tin lỗi hoặc cập nhật cho các routes, thiết bị trung gian hoặc máy chủ khác. IPv4 được sử dụng rộng rãi (Giao thức Internet phiên bản 4), còn IPv6 mới hơn sử dụng các phiên bản tương tự của giao thức ICMP (ICMPv4 và ICMPv6 tương ứng).

## 4.2. NỘI DUNG THỰC HÀNH

### 4.2.1. Cấu hình máy tính

1. Tạo mạng Lan có sơ đồ mạng như hình vẽ
2. Thực hiện cấu hình địa chỉ IP cho các máy tính như hình vẽ.
3. Trên máy tính 192.168.1.2 thực hiện kết nối với switch sử dụng công cụ ssh



#### **4.3. BÁO CÁO BÀI THỰC HÀNH SỐ 2**

Họ và tên sinh viên: MSSV:

Mã lớp thực hành: Mã lớp lý thuyết:

Địa chỉ IP của máy tính trong quá trình thực hành:

#### **Thực hành demo (3 điểm)**

Sinh viên kết nối vào switch và ghi lại thông tin bảng địa chỉ MAC trên các cổng kết nối tới PC1, PC3 tại các thời điểm trước và sau khi thực hiện gửi gói tin từ máy tính PC1 đến máy tính PC3 và ngược lại.

Lệnh xem thông tin bảng địa chỉ MAC trên 1 cổng (ví dụ Gi0/3) như sau:

**c2960#sh mac address-table interface Fa0/1**

Mac Address Table

```
-----  
Vlan Mac Address Type Ports  
--- --- --- ---  
32 68b5.99fc.d1df DYNAMIC Fa0/1
```

Total Mac Addresses for this criterion: 1

Với sơ đồ mạng LAN ở mục 4.2.1, sinh viên điền kết quả thực hiện vào bảng theo mẫu dưới đây cho các trường hợp:

1. PC1 ping PC2
2. PC2 ping PC3
3. PC3 ping PC4

Cổng	Trước khi ping PC1->PC2	Sau khi ping PC1->PC2
Fa0/1	Rỗng	MAC: 68b5.99fc.d1df Port: Fa0/1 MAC: 001b.10ae.7d00 Port: Fa0/2

## **5. BÀI THỰC HÀNH SỐ 3: ĐỊNH TUYẾN TĨNH TRONG MẠNG IP**

### **5.1 MỤC ĐÍCH VÀ NỘI DUNG**

#### **5.1.1. Mục đích**

Với bài thực hành này, Sinh viên được trang bị kỹ năng thực hành về định tuyến nội vùng để có thể cấu hình định tuyến tĩnh cho các mạng máy tính sử dụng các router IP sao cho các mạng có thể truyền dữ liệu cho nhau và có thể kết nối Internet. Cụ thể, sinh viên thực hành về địa chỉ IP, bảng định tuyến, sử dụng các công cụ, câu lệnh cấu hình và kiểm tra kết nối.

#### **5.1.2. Yêu cầu đối với sinh viên**

- Kiến thức lý thuyết:  
Sinh viên nắm vững nguyên lý định tuyến trong mạng IP, nguyên tắc hoạt động dựa trên bảng định tuyến của các router, nguyên tắc thiết lập bảng định tuyến, nguyên tắc gán địa chỉ IP.
- Kỹ năng thực hành:
  - o Sinh viên có khả năng kết nối các thiết bị mạng switch, router để tạo thành các mạng con kết nối với nhau
  - o Sinh viên thiết lập thành thạo bảng định tuyến tĩnh sử dụng chức năng router của Linux.
- **Nội dung cần nộp cuối buổi thực hành:**
  - o Demo cho trợ giảng các bước kiểm tra kết nối cuối các phần 5.2.1, 5.2.2. Phần demo chiếm 1 điểm/10.
  - o Báo cáo (bản giấy) theo mẫu đã cung cấp. Phần báo cáo gồm các câu trả lời cho các câu hỏi, chiếm 9 điểm/10.

#### **5.1.3. Cơ sở lý thuyết**

##### **5.1.3.1 Địa chỉ IP**

Để phân biệt các máy tính trên Internet, mỗi máy được gán một địa chỉ IP. Địa chỉ IP (version 4) gồm 4 byte, ví dụ 10000010 10001010 00001000 00000001.

Để thuận tiện sử dụng, địa chỉ IP được viết dưới dạng 4 số thập phân cách nhau dấu chấm, ví dụ, địa chỉ trên được viết thành: 130.238.8.1.

Mỗi địa chỉ IP của một nút mạng gồm 2 phần, các bit định danh mạng (network ID, nằm bên trái), xác định mạng nào nút đang được nối vào và các bit định danh máy (hostID, nằm bên phải) xác định một trạm duy nhất trong mạng.

Vị trí danh giới giữ các bit định danh mạng và định danh máy không cố định. Để xác định danh giới này, người ta có thể áp dụng một trong 2 nguyên tắc:

- Phân lớp địa chỉ thành các lớp A, B, C, D, E (xem lại bài giảng), hoặc
- Không phân lớp địa chỉ và sử dụng mặt nạ. Mặt nạ là con số cho biết bao nhiêu bit trái nhất thuộc về phần định danh mạng.

Ví dụ, mặt nạ mạng có thể là 24, xác định 24 bit bên trái nhất thuộc định danh mạng. Mặt nạ mạng cũng có thể được viết dưới dạng 32 bit như địa chỉ IP với các bit thuộc phần định danh mạng bằng 1 và các bit thuộc phần định danh máy bằng 0.

Ví dụ mặt nạ 24 được viết thành 11111111 11111111 11111111 0000000,

hoặc cũng có thể viết dưới dạng thập phân như địa chỉ IP thành 255.255.255.0.

Với mặt nạ 24 số bit dành cho định danh máy là  $32-24=8$  bit. Như vậy, mạng sử dụng mặt nạ này có tối đa  $2^8 = 256$  địa chỉ IP phân biệt. Loại trừ 2 địa chỉ IP đặc biệt: địa chỉ mạng với toàn bit 0 phần hostID và địa chỉ broadcast với toàn bit 1 phần hostID thì còn lại 254 địa chỉ có thể dùng gán cho các máy.

### **5.1.3.2. Kết nối liên mạng và định tuyến**

Internet bao gồm nhiều mạng LAN nhỏ nối với nhau. Để chuyển dữ liệu giữa các mạng LAN này, cần có một cơ chế chuyển tiếp dữ liệu. Cơ chế đó trong mạng IP là cơ chế IP forwarding được thực hiện bởi các router IP nằm trung gian kết nối giữa các mạng LAN.

Một router là một nút mạng về cơ bản có ít nhất 2 giao diện nối với (thuộc về) 2 mạng LAN khác nhau. Router nhận gói tin IP từ một giao diện và chuyển tiếp gói tin sang một trong các giao diện còn lại tùy vào địa chỉ đích của gói tin, sao cho gói tin hướng đến mạng đích. Để làm được như vậy, đầu tiên phải xác định được đường đi cho các gói tin từ mọi nguồn đến mọi đích. Kết quả các đường đi này được ghi vào các router dưới dạng bảng định tuyến (routing table).

Bảng định tuyến phải được xây dựng căn cứ vào topology của mạng. Bảng định tuyến phải được cập nhật thường xuyên phản ánh các thay đổi topogoly trong mạng. Trong mạng nhỏ, đơn giản, bảng định tuyến có thể được xây dựng thủ công (định tuyến tĩnh), hoặc xây dựng bằng các giao thức định tuyến một cách tự động. Một số giao thức định tuyến phổ biến: Routing Information Protocol (RIP) và Open Shortest Path First (OSPF).

### **5.1.3.3. Bảng định tuyến và câu lệnh cấu hình**

Bảng định tuyến gồm nhiều dòng với cấu trúc:

[Destination, netmask, cost, next hop, interface]

Ví dụ:

169.254.0.0	255.255.0.0	1000	0.0.0.0	eth0
192.168.6.0	255.255.255.0	0	0.0.0.0	eth1
192.168.122.0	255.255.255.0	0	0.0.0.0	eth2
0.0.0.0	0.0.0.0	0	0.0.0.0	eth2

Khi có một gói tin đến router với địa chỉ đích Y, router thực hiện tính toán với mỗi dòng của bảng định tuyến xem địa chỉ Y với mặt nạ của dòng có thuộc mạng đích của dòng hay không? Nếu đúng thì dòng được coi là phù hợp. Nếu có nhiều dòng phù hợp thì nguyên tắc “Longest matching” được áp dụng, theo đó, dòng tương ứng với mạng đích có số bít phù hợp với địa chỉ IP của Y dài nhất được chọn.

Nếu không có dòng nào phù hợp, đường đi mặc định được áp dụng. Đường đi mặc định có địa chỉ mạng và mặt nạ gồm toàn 0. Nếu không có đường đi mặc định, gói tin sẽ bị bỏ.

Trong hệ thống Linux, các giao diện mạng Ethernet thường được đặt tên là ethX với X là các số tăng dần từ 0. Ví dụ, giao diện mạng đầu tiên được gọi là eth0, giao diện tiếp theo được gọi là eth1, v.v... Một số trường hợp giao diện mạng cũng có thể có tên khác.

*Để xem tên của các giao diện/cổng mạng có trên máy*

```
$ ifconfig
```

*Câu lệnh kích hoạt, cấu hình, đặt địa chỉ IP v.v... cho một giao diện mạng*

```
$ ifconfig
```

*Ví dụ:*

```
$ ifconfig eth0 192.168.200.1 netmask 255.255.255.0 up
```

*Câu lệnh này bật giao diện mạng eth0 và gán cho nó địa chỉ 192.168.200.1/24*

*Câu lệnh hiển thị và truy cập bảng định tuyến.*

```
$ route
```

*Ví dụ, thêm một đường đi cụ thể đến mạng 192.168.205.0 bằng cách chuyển dữ liệu đến nút mạng tiếp theo có địa chỉ 192.168.200.1 được kết nối trực tiếp với máy qua một giao diện mạng.*

```
$ sudo route add -net 192.168.205.0 netmask 255.255.255.0 gw  
192.168.200.1
```

*Để thêm một đường đi mặc định đến mọi mạng bằng cách chuyển dữ liệu đến nút mạng tiếp theo có địa chỉ 10.1.0.1 được kết nối trực tiếp với máy qua một giao diện mạng.*

```
$ sudo route add default gw 10.1.0.1
```

*Xem lại bảng định tuyến*

```
$ route -n
```

*Câu lệnh in đường đi của một gói tin đến một host*

```
$ traceroute
```

*Ví dụ:*

```
$ traceroute -n -z 1 192.168.205.1
```

*Câu lệnh xem và thiết lập chức năng IP forward của máy*

```
$ sudo sysctl net/ipv4/ip_forward
```

```
$ sudo sysctl -w net.ipv4.ip_forward=1
```

*Câu lệnh này bật chức năng IP forwarding trên linux biến máy thành 1 router*

*Câu lệnh cài đặt DHCP server*

```
$ sudo apt install isc-dhcp-server
```

*Câu lệnh thiết lập dịch vụ DHCP server trên router*

Chỉnh sửa file cấu hình /etc/dhcp/dhcpd.conf

```
authoritative;
```

```
subnet 10.1.1.0 netmask 255.255.255.0 {  
    range 10.1.1.101 10.1.1.200;  
    option routers 10.1.1.2; }
```

Trong đó các thông tin tương ứng:

Network: 10.1.1.0

Subnet: 255.255.255.0

DCHP Range: 10.1.1.101 – 10.1.1.200

Mục option đặc tả thông tin sẽ được đẩy về cho máy chạy DHCP client. Ví dụ “option routers” đặc tả gateway/router sẽ được thiết lập cho máy nhận cấu hình từ DHCP. Các mục option này không nhất thiết phải có.

*Khởi động lại dịch vụ DHCP server để áp dụng cấu hình trên bằng lệnh:*

```
sudo systemctl restart isc-dhcp-server.service
```

*Kiểm tra danh mục các máy đang nhận IP động từ máy chạy DHCP server*

```
$ dhclient -lease-list
```

Thu được danh sách tương tự như sau:

```
To get manufacturer names please download
```

```
http://standards.ieee.org/regauth/oui/oui.txt to /usr/local/etc/oui.txt
```

```
Reading leases from /var/lib/dhcp/dhcpd.leases
```

MAC	IP	hostname	valid until
manufacturer			

```
=====
00:0c:29:45:ba:4d  10.1.1.135      DESKTOP-8UK989 2019-12-12 13:22:00 -
NA-
```

#### *Câu lệnh bật dịch vụ DHCP trên client*

```
$ sudo dhclient -r eth0
```

*Lệnh trên bật dịch vụ DHCP client trên máy chạy lệnh, giao diện eth0*

Sử dụng trình man để xem thêm hướng dẫn sử dụng các câu lệnh trên.

Lưu ý: Từ gateway nói chung dùng để chỉ một router là điểm vào/ra của một mạng.

## **5.2 NỘI DUNG THỰC HÀNH**

Sinh viên được chia thành nhóm 4 sinh viên.

Mỗi nhóm được cung cấp 3 Rasbery PI để làm router, 3 switch để tạo 3 mạng LAN, 3 máy tính để làm 3 workstations và 6 USB Ethernet để bổ sung cổng mạng cho PI.

### **5.2.1. Kết nối hai mạng LAN sử dụng router**

Một công ty có 2 trụ sở ở Sài gòn và Hà nội (xem hình). Mỗi trụ sở có một mạng LAN. Mỗi mạng LAN có vài máy trạm nhưng bạn chỉ được truy cập vào 2 máy có tên hn-workstation ở Hanoi, và sg-workstation ở Sài gòn và các router hn-router và sg-router ở mỗi mạng LAN.

Mỗi LAN có thể được dùng để giao tiếp trong trụ sở nhưng không thể giao tiếp được với trụ sở phía bên kia. Để 2 trụ sở có thể giao tiếp với nhau, một đường cáp thuê riêng (leased line) được thiết lập giữa 2 trụ sở Saigon và Hanoi.

Mạng Sài gòn được cung cấp dải địa chỉ IP 10.1.0.0 với mặt nạ 255.255.0.0. Tương tự, mạng Hà nội được cung cấp dải địa chỉ IP 10.2.0.0 và cũng sử dụng mặt nạ 255.255.0.0.

Các host trong cùng một mạng có NetID giống nhau và có thể giao tiếp trực tiếp với nhau.

Với một địa chỉ IP và một mặt nạ mạng, ta có thể xác định được địa chỉ của mạng chứa địa chỉ IP này.

#### **5.2.1.1 Hoạch định địa chỉ IP**

**Câu hỏi 1 (1 điểm):** Gán địa chỉ IP phù hợp cho các trạm sg-workstation, hn-

workstation và các giao diện của các router và điền các địa chỉ này lên sơ đồ mạng

Địa chỉ IP hn-workstation: ..... Mặt  
nạ:.....

Địa chỉ IP sg-workstation: ..... Mặt  
nạ:.....

Địa chỉ router Hanoi-eth0: ..... Mặt  
nạ:.....

Địa chỉ router Hanoi-eth1: ..... Mặt  
nạ:.....

Địa chỉ router Saigon-eth0: ..... Mặt  
nạ:.....

Địa chỉ router Saigon-eth1: ..... Mặt  
nạ:.....

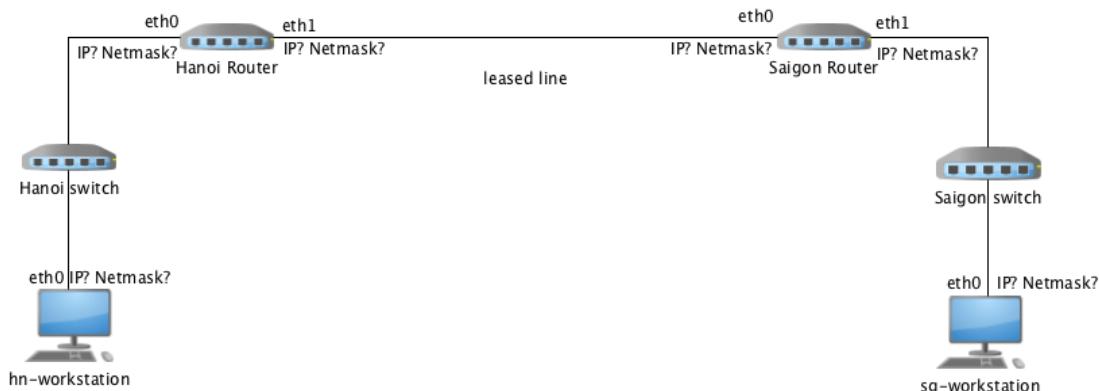


Figure 1: Sơ đồ mạng

### 5.2.1.2 Kết nối và cấu hình

Mục tiêu của phần thực hành là kết nối mạng theo sơ đồ Figure 1 và cấu hình sao cho các trạm có thể nói chuyện với nhau. Để làm được như vậy, sinh viên cần thực hiện cấu hình theo các bước sau.

Lưu ý: Để làm được bài thực hành này, sinh viên cần có quyền quản trị khi thực hiện các câu lệnh (quyền root hoặc dùng lệnh sudo)

**Bước 1:** Nối các thiết bị theo sơ đồ Figure 1.

**Bước 2:** Cấu hình các máy trạm. Công việc cần làm trong bước này gồm:

- Thiết lập địa chỉ IP cho máy trạm.

- Thiết lập luật định tuyến cho máy trạm. Trên máy trạm, ta cần bảo cho máy biết với các địa chỉ đích thuộc cùng mạng thì có thể chuyển dữ liệu trực tiếp không qua router. Thông thường luật này được thêm tự động vào bảng định tuyến mỗi khi bật một giao diện mạng. Có thể sử dụng lệnh route -n để kiểm tra bảng định tuyến
- Với các địa chỉ đích không thuộc cùng mạng thì cần phải chuyển các gói tin đến router của mạng để được định tuyến tiếp. Có 2 lựa chọn i) thêm một đường đi tĩnh đến mỗi mạng đích, hoặc ii) thêm một đường đi mặc định đến cả mạng đích nếu đường đi đến mọi mạng đích đều như nhau. Trong bài thí nghiệm này, hãy sử dụng đường đi tĩnh vì chúng ta sẽ mở rộng mạng trong phần tiếp theo.

**Câu hỏi 2 (1 điểm):** Bật các giao diện mạng trên máy trạm và gán địa chỉ IP như đã định ra trong Câu hỏi 1 bằng cách sử dụng câu lệnh ifconfig. Câu lệnh cần dùng với mỗi máy trạm là:

Máy trạm Hà nội:

.....

Máy trạm Sài gòn:

.....

**Câu hỏi 3 (1 điểm):** Thiết lập luật định định tuyến trên máy trạm.

Sử dụng lệnh route -n để kiểm tra bảng định tuyến

Sử dụng lệnh route add để thêm một đường đi tĩnh đến mạng ở xa. Thực hiện câu lệnh trên **hn-workstation** để định tuyến đến mạng Sài gòn:

.....

Thực hiện câu lệnh cần chạy trên máy **sg-workstation** để định tuyến đến mạng Hà nội:

.....

### Bước 3: Cấu hình các router:

- Thiết lập IP cho các router. Mỗi router có 2 giao diện cần cấu hình: giao diện nối với mạng LAN và giao diện nối với router ở xa.  
Giao diện router nối với mỗi mạng LAN phải có địa chỉ IP thuộc dải của mạng LAN.  
Hai giao diện của 2 router nối với nhau trên đường leased line có thể có địa chỉ tùy ý nhưng chúng phải có thuộc cùng một mạng. Tức là địa chỉ IP của chúng phải có cùng địa chỉ mạng.

**Câu hỏi 4 (1 điểm):** Thực hiện câu lệnh thiết lập địa chỉ IP cho các giao diện nối với mạng LAN của router Hà nội :

và router Sài gòn:

Thực hiện câu lệnh thiết lập địa chỉ IP cho các giao diện nối với đường leased line của router Hà nội :

và router Sài gòn:

- Thiết lập luật định tuyến cho các router để chúng thực hiện chuyển tiếp gói tin giữa 2 mạng LAN.

**Câu hỏi 5 (1 điểm):** Thực hiện câu lệnh trên router Hà nội để thêm luật định tuyến đến mạng Sài gòn:

Thực hiện câu lệnh trên router Sài gòn để thêm luật định tuyến đến mạng Hà nội:

Lưu ý: Trong bài thí nghiệm này, ta dùng các máy Linux để làm router, vì thế cần kích hoạt chức năng chuyển tiếp IP của Linux bằng cách thực hiện lệnh sau trên mỗi router.

`$ sysctl -w net.ipv4.ip_forward=1` – to enable IP forwarding.

**Bước 4 (0.5 điểm):** Kiểm tra kết nối (*cần demo với trợ giảng*)

Đến lúc này nếu các cấu hình đều đúng thì các máy ở các mạng đã có thể chuyển dữ liệu cho nhau. Sử dụng lệnh traceroute để kiểm tra tính thông suốt của các kết nối giữa máy trạm hn-workstation và sg-workstation. Kết quả có thể tương tự như sau:

```
sg-workstation:~# traceroute -n -z 1 10.2.0.10
traceroute to 10.2.0.10 (10.2.0.10), 30 hops max, 38 byte
packets
1 10.1.0.1 2.600 ms 0.831 ms 0.802 ms
2 10.10.0.2 3.517 ms 1.161 ms 1.156 ms
```

```
3 10.2.0.10 7.695 ms 1.528 ms 1.514 ms  
sg-workstation:~#
```

Cần đảm bảo kết nối được thông suốt trước khi thực hiện phần tiếp theo của bài thực hành.

### 5.2.2 Dịch vụ DHCP và Kết nối đến Internet

Công ty muốn kết nối đến một nhà cung cấp dịch vụ Internet (ISP) tại Hà nội để cung cấp khả năng truy cập ra bên ngoài cho các máy của công ty. Vì một lý do nào đó, công ty chỉ muốn duy trì duy nhất một kết nối đến ISP này. Để cả 2 văn phòng cùng truy cập được ISP, các luồng dữ liệu phải được định tuyến qua Hà nội. Để nối như vậy, tại router Hà nội, một giao diện mạng eth2 được bổ sung, giao diện này sẽ nối trực tiếp với Router của ISP và router này một mặt đã được ISP nối đến Internet. Xem Hình 3.

Để thuận tiện cho việc mở rộng sau này, công ty muốn thiết lập để Router ISP cấp phát địa chỉ IP động cho tất cả các giao diện kết nối đến nó bằng dịch vụ DHCP. Như vậy sau này khi muốn nối thêm router nào với Router ISP thì router ấy cũng sẽ nhận được địa chỉ IP tự động. Công ty cũng muốn địa chỉ IP động sẽ sử dụng dải:

Dải IP: 192.168.N.0

Netmask: 255.255.255.0

Địa chỉ IP của router ISP (giao diện nối với mạng Hà nội) được cố định là 192.168.N.1

Trong đó N là số của Nhóm thực hành mà các bạn đang đăng ký. Ví dụ nếu bạn đăng ký nhóm thực hành là N03 thì dải IP dùng là 192.168.3.0/24

Công ty nhờ bạn cấu hình Router ISP để kích hoạt dịch vụ DHCP. Sau đó, bạn cần giúp công ty nối router Hà nội với router ISP và thực hiện điều chỉnh cần thiết để tất cả các luồng dữ liệu đến Internet từ cả mạng Hà nội, Sài gòn đều được định hướng sang Router ISP.

Cụ thể các công việc cần làm như sau

**Bước 1:** Cấu hình và bật dịch vụ DHCP Server trên Router ISP để nó cấp phát IP trong dải trên và bật dịch vụ DHCP client trên giao diện của Router Hà nội nối với Router ISP

**Câu hỏi 6 (1 điểm):** Viết nội dung cấu hình cần có trong /etc/dhcp/dhcpd.conf

```
.....  
.....  
.....  
.....  
.....
```

Viết câu lệnh kích hoạt dịch vụ DHCP trên Router ISP

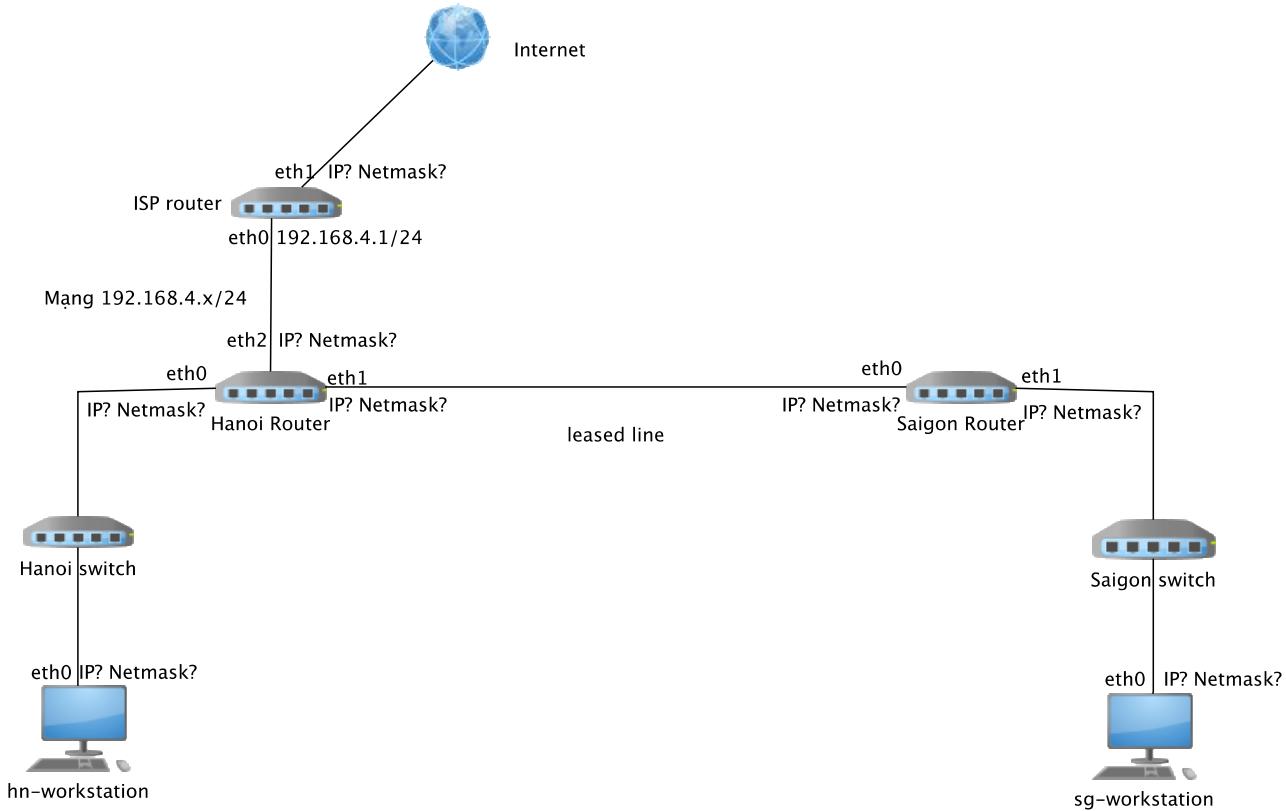


Figure 2: Mạng với kết nối Internet tại chi nhánh Hà nội

**Câu hỏi 7 (1 điểm):** Viết câu lệnh kích hoạt dịch vụ DHCP trên Router Hà nội để nó nhận IP tự động từ router ISP

Địa chỉ IP mà Router Hà nội nhận được trên giao diện eth2 là gì

**Bước 2:** Cấu hình router Hà nội, Sài gòn

**Câu hỏi 8 (1 điểm):** Điều chỉnh bảng định tuyến của router Hà nội để chuyển tiếp dữ liệu không hướng vào các mạng LAN Hà nội, Sài gòn ra Internet. Nên sử dụng đường

đi mặc định

.....

.....

Điều chỉnh bảng định tuyến của router Sài gòn để chuyển tiếp dữ liệu ra Internet qua router Hà nội. Nên sử dụng đường đi mặc định

.....

.....

**Câu hỏi 9 (1 điểm):** Cấu hình định tuyến trên router ISP để nó có thể chuyển tiếp dữ liệu tới các mạng tại Hà Nội, Sài Gòn.

.....

.....

.....

.....

**Bước 4 (0.5 điểm):** Kiểm tra kết nối (*cần demo với trợ giảng*)

Đến lúc này nếu các cấu hình đều đúng thì các máy ở các mạng đã có thể chuyển dữ liệu cho nhau.

Gán địa chỉ IP 100.100.100.1 cho một giao diện ngoài của ISP Router (giao diện không nối với Router Hà nội, eth1 trên hình). Nếu các máy trong mạng có thể truyền dữ liệu đến giao diện này thì coi như chúng truyền dữ liệu được ngoài Internet.

Sử dụng lệnh traceroute để kiểm tra tính thông suốt của các kết nối ra Internet (qua địa chỉ 100.100.100.1) từ các máy trạm tại Hà nội, Sài gòn.

### 1.3. BÁO CÁO BÀI THỰC HÀNH SỐ 3

Họ và tên sinh viên:

MSSV:

Mã lớp thực hành:

Mã lớp lý thuyết:

#### 5.3.1 Kết nối hai mạng LAN sử dụng router

**Câu hỏi 1 (1 điểm):** Gán địa chỉ IP phù hợp cho các trạm sg-workstation, hn-workstation và các giao diện của các router và điền các địa chỉ này lên sơ đồ mạng

Địa chỉ IP hn-workstation: ..... Mặt nạ: .....

Địa chỉ IP sg-workstation: ..... Mặt nạ: .....

Địa chỉ router Hanoi-eth0: ..... Mặt nạ: .....

Địa chỉ router Hanoi-eth1: ..... Mặt nạ: .....

Địa chỉ router Saigon-eth0: ..... Mặt nạ: .....

Địa chỉ router Saigon-eth1: ..... Mặt nạ: .....

*Điền các địa chỉ lên sơ đồ mạng.*

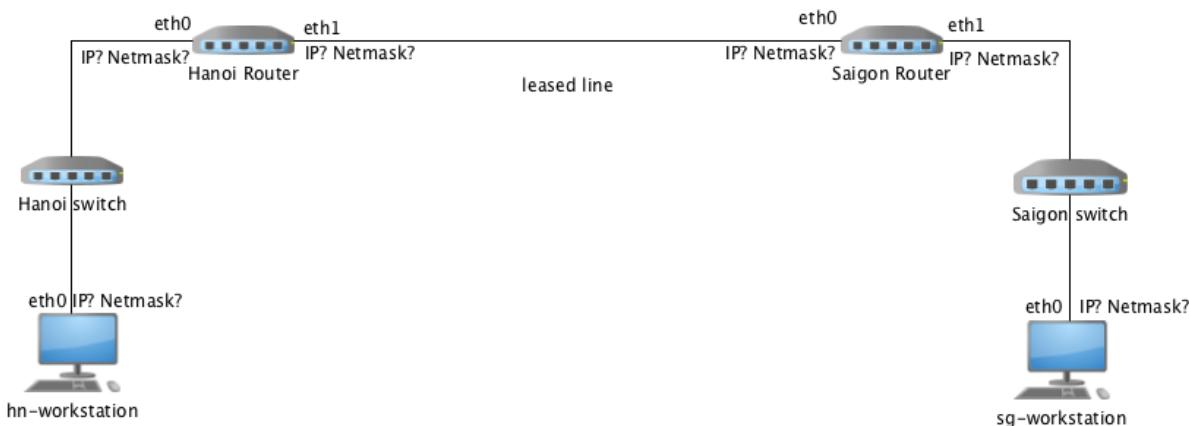


Figure 3: Sơ đồ mạng.

**Câu hỏi 2 (1 điểm):** Bật các giao diện mạng trên máy trạm và gán địa chỉ IP như đã định ra trong Câu hỏi 1 bằng cách sử dụng câu lệnh ifconfig. Câu lệnh cần dùng với mỗi máy trạm là:

Máy trạm Hà nội:

.....

Máy trạm Sài gòn:

**Câu hỏi 3 (1 điểm):** Thiết lập luật định định tuyến trên máy trạm.

Sử dụng lệnh `route -n` để kiểm tra bảng định tuyến

Sử dụng lệnh `route add` để thêm một đường đi tĩnh đến mạng ở xa. Thực hiện câu lệnh trên **hn-workstation** để định tuyến đến mạng Sài gòn:

Thực hiện câu lệnh cần chạy trên máy **sg-workstation** để định tuyến đến mạng Hà nội:

**Câu hỏi 4 (1 điểm):** Thực hiện câu lệnh thiết lập địa chỉ IP cho các giao diện nối với mạng LAN của router Hà nội :

và router Sài gòn:

Thực hiện câu lệnh thiết lập địa chỉ IP cho các giao diện nối với đường leased line của router Hà nội :

và router Sài gòn:

**Câu hỏi 5 (1 điểm):** Thực hiện câu lệnh trên router Hà nội để thêm luật định tuyến đến mạng Sài gòn:

Thực hiện câu lệnh trên router Sài gòn để thêm luật định tuyến đến mạng Hà nội:

### 5.3.2 Dịch vụ DHCP và Kết nối đến Internet

**Câu hỏi 6 (1 điểm):** Viết nội dung cấu hình cần có trong `/etc/dhcp/dhcpd.conf`

.....  
.....  
.....

Viết câu lệnh kích hoạt dịch vụ DHCP trên Router ISP

.....  
.....

**Câu hỏi 7 (1 điểm):** Viết câu lệnh kích hoạt dịch vụ DHCP trên Router Hà nội để nó nhận IP tự động từ router ISP

.....  
.....

Địa chỉ IP mà Router Hà nội nhận được trên giao diện eth2 là gì

.....  
.....

**Câu hỏi 8 (1 điểm):** Điều chỉnh bảng định tuyến của router Hà nội để chuyển tiếp dữ liệu không hướng vào các mạng LAN Hà nội, Sài Gòn ra Internet. Nên sử dụng đường đi mặc định

.....  
.....

Điều chỉnh bảng định tuyến của router Sài Gòn để chuyển tiếp dữ liệu ra Internet qua router Hà nội. Nên sử dụng đường đi mặc định

.....  
.....

**Câu hỏi 9 (1 điểm):** Cấu hình định tuyến trên router ISP để nó có thể chuyển tiếp dữ liệu tới các mạng tại Hà Nội, Sài Gòn.

.....  
.....  
.....  
.....

## **2. BÀI THỰC HÀNH SỐ 4: BÀI THỰC HÀNH SỐ 4: PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC UDP VÀ TCP**

### **6.1. MỤC ĐÍCH VÀ NỘI DUNG**

#### **6.1.1. Mục đích**

Bài thí nghiệm này được thiết kế để trang bị cho sinh viên các kỹ năng sử dụng phần mềm Wireshark để bắt và lọc các gói tin UDP, TCP theo yêu cầu. Thông qua đó, sinh viên có thể quan sát và hiểu được các hoạt động quan trọng của hai giao thức này. Bên cạnh đó, thông qua việc vận dụng kiến thức lý thuyết, sinh viên có thể thực hiện các tính toán, giải thích kết quả đã quan sát được.

#### **6.1.2. Yêu cầu đối với sinh viên**

- Môi trường thực hành:
  - Sử dụng thành thạo các chức năng cơ bản của phần mềm Wireshark
  - Thực hiện thành thạo các thao tác trên hệ điều hành Windows, bao gồm các thao tác với thông số TCP/IP đã được hướng dẫn trong các bài thực hành trước.
- Kiến thức: Nắm vững kiến thức về tầng giao vận, các giao thức UDP và TCP.
- Viết báo cáo thực hành và nộp kết quả theo yêu cầu như sau:
  - Báo cáo(bản giấy) theo mẫu đã cung cấp
  - File lưu lượng **lab04.pcapng**(Kích thước không quá 1 MB) đặt trong thư mục có tên định dạng **TenSV\_MSSV\_Lab04**. Nén thư mục và gửi vào địa chỉ email theo yêu cầu của cán bộ hướng dẫn thực hành.

#### **6.1.3. Cơ sở lý thuyết**

##### **6.1.3.1. Giao thức UDP**

UDP (User Datagram Protocol) là một trong hai giao thức điều khiển truyền dữ liệu trên tầng giao vận trong mô hình TCP/IP. UDP hoạt động theo nguyên lý truyền thông hướng không liên kết(connectionless protocol). Theo đó, giao thức UDP nhận dữ liệu từ tiến trình của tầng ứng dụng, đóng gói vào các UDP datagram(gói tin UDP) và gửi ngay tới phía đích mà không cần thiết lập liên kết. Các gói tin UDP sẽ được phía đích nhận và xử lý một cách độc lập. Nếu gói tin không có lỗi, UDP sẽ chuyển lên cho tiến trình tương ứng của tầng ứng dụng; ngược lại nó sẽ hủy gói tin.Thêm vào đó, dù trong trường hợp nào đi chăng nữa, sẽ không có một gói tin báo nhận được gửi trả lại cho phía đích. Điều này dẫn đến một trong những đặc điểm quan trọng khác của UDP là

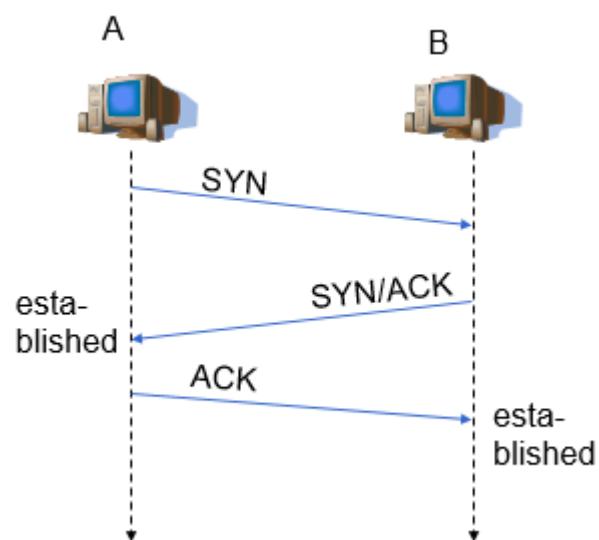
truyền thông không tin cậy, nghĩa là quá trình điều khiển của UDP không đảm bảo truyền dữ liệu tới đích thành công. Nói một cách khác, phía nguồn chỉ truyền dữ liệu một lần và không cần biết dữ liệu có được truyền đi thành công hay không. Chế độ truyền như vậy được gọi là chế độ best-effort. Bên cạnh đó, UDP sẽ thực hiện truyền liên tục dữ liệu với tốc độ cao nhất có thể. Điều này có thể gây tăng nguy cơ xảy ra tắc nghẽn trên đường truyền hoặc làm phía đích quá tải, không thể xử lý kịp thời dữ liệu nhận được.

### 6.1.3.2. Giao thức TCP

TCP (Transmission Control Protocol) là giao thức có cách hoạt động rất phức tạp so với UDP. Trước hết, TCP tuân theo nguyên lý của truyền thông hướng liên kết (connection-oriented), trong đó quá trình truyền gồm 3 giai đoạn: thiết lập liên kết, truyền dữ liệu và đóng liên kết. Để phục vụ việc quản lý và thông báo trạng thái liên kết giữa các bên, giao thức TCP thiết kế gói tin với các cờ điều khiển trong phần tiêu đề.

Ý nghĩa của quá trình thiết lập liên kết trong giao thức TCP là phía nguồn chỉ gửi dữ liệu khi nào phía đích đã sẵn sàng. Quá trình này thực hiện theo giao thức bắt tay 3 bước (three-handshake protocol):

- Bước 1: Phía yêu cầu(A) gửi một gói tin TCP không có phần thân(payload), có cờ SYN trong tiêu đề gói tin được bật.
- Bước 2: Nếu phía đáp ứng(B) sẵn sàng thiết lập liên kết, nó gửi gói tin với hai cờ SYN và ACK được bật. Gói tin này cũng không có phần thân.
- Bước 3: Phía yêu cầu gửi gói tin với cờ ACK được bật để xác nhận liên kết đã được thiết lập. Gói tin này có thể có phần payload.



Trên liên kết đã được thiết lập, dữ liệu của tiến trình tầng ứng dụng chuyển xuống được TCP đóng gói thành các TCP segment (gói tin TCP) và truyền đi bằng kỹ thuật truyền dòng (byte stream). Trong kỹ thuật này, phía nguồn sẽ đánh số thứ tự (Sequence Number) cho các gói tin gửi đi, còn phía nhận nếu cần sẽ sắp xếp các gói tin này theo đúng thứ tự và hợp lại thành một thông điệp gửi lên cho tiến trình tầng ứng dụng. Với cách truyền như vậy, rất có thể một thông điệp này sẽ đính theo dữ liệu

của các thông điệp khác, tức là biên của các thông điệp là không rõ ràng. Các tiến trình của tầng ứng dụng phải sử dụng một cách thức nào đó để phân tách các thông điệp.

Bên cạnh đó, TCP là một giao thức truyền thông tin cậy. Phía gửi luôn biết rằng dữ liệu mà nó truyền đi có được truyền thành công hay không. Bởi vì giao thức TCP quy định rằng phía đích phải gửi gói tin báo nhận cho phía nguồn với cờ ACK được bật. Trong tiêu đề của gói tin này, giá trị ACK Number cho biết số thứ tự của dữ liệu mà phía đích cần nhận. Nếu phía nguồn xác định có lỗi xảy ra, dữ liệu trước đó sẽ được gửi lại; ngược lại dữ liệu tiếp theo được gửi đi. Sau khi hoàn thành việc truyền dữ liệu, các bên thực hiện các thao tác thỏa thuận đóng liên kết một cách tin cậy bằng cách gửi gói tin có cờ FIN được bật và để chắc chắn tất cả dữ liệu đã được nhận thành công.

Cuối cùng, để quá trình truyền không làm tắc nghẽn đường truyền và quá tải cho phía đích, giao thức TCP sử dụng cơ chế điều khiển tắc nghẽn và điều khiển luồng để giới hạn kích thước dữ liệu được gửi đi trong một lần truyền.

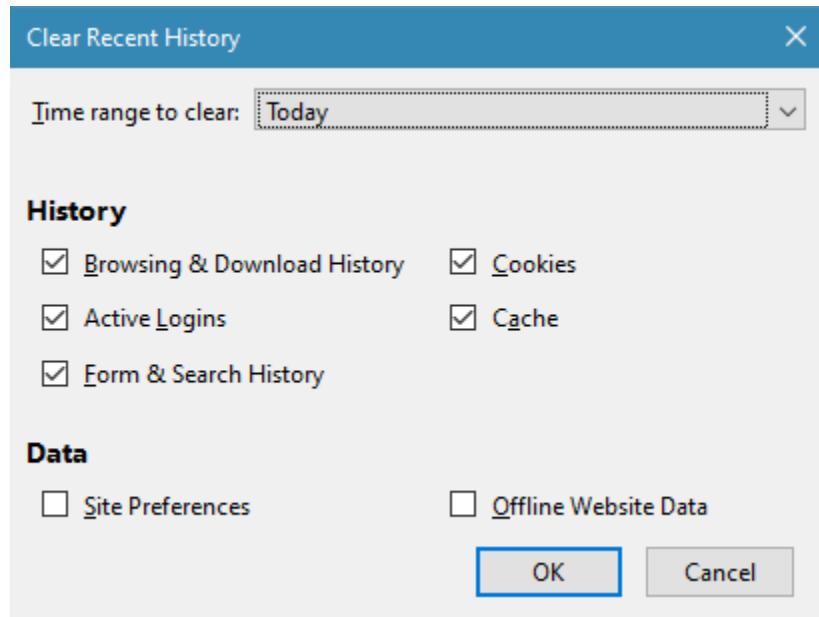
## 6.2. NỘI DUNG THỰC HÀNH

### 6.2.1. Xác định thông số của máy trạm

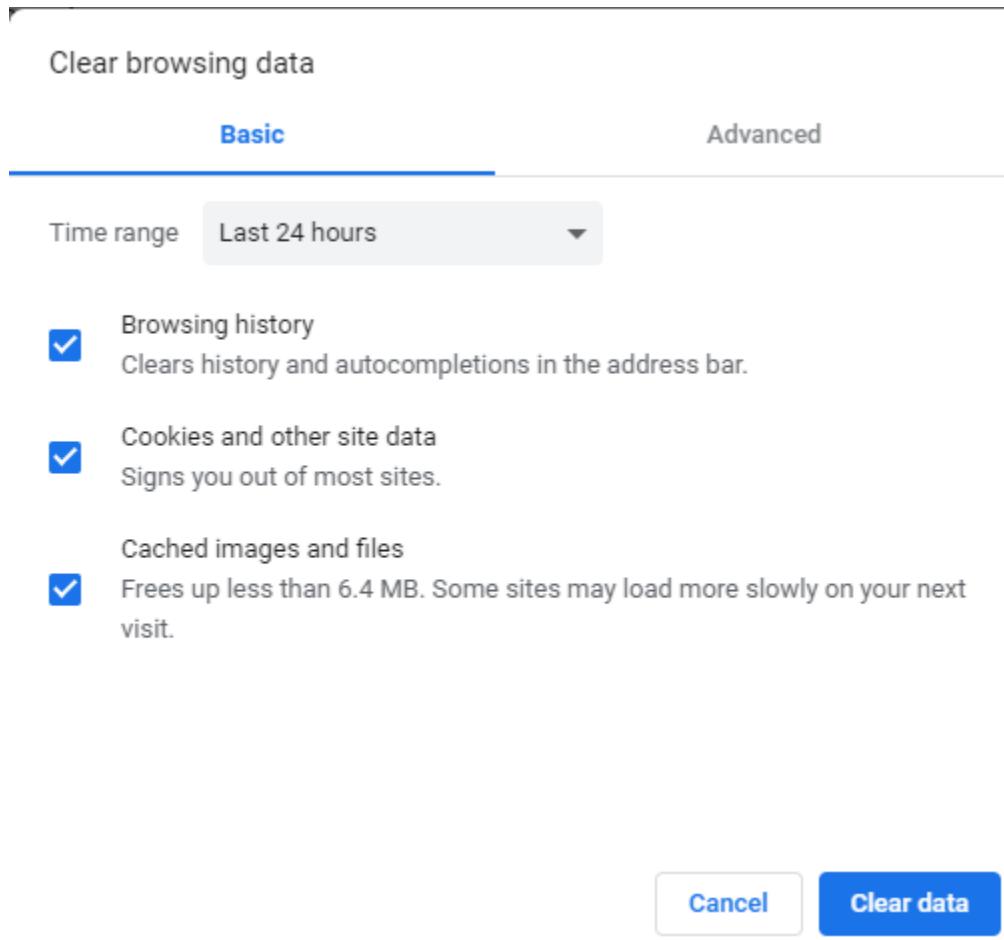
Sinh viên xác định địa chỉ IP trên máy tính ở phòng thực hành và ghi vào báo cáo. Để có được thông tin này, sinh viên xem lại bài thực hành số 2 và 3.

### 6.2.2. Thu thập lưu lượng mạng

- **Bước 1:** Tắt các chương trình của người dùng có trao đổi dữ liệu trên mạng trừ trình duyệt Web để có thể quan sát quá trình truyền dữ liệu dưới đây một cách tốt nhất.
- **Bước 2:** Download file sau: <http://nct.soict.hust.edu.vn/mmt/alice.txt>
- **Bước 3:** Trên cửa sổ trình duyệt Web, truy cập vào địa chỉ:  
<http://nct.soict.hust.edu.vn/mmt/lab04/>
- **Bước 4:** Xóa bộ đệm của trình duyệt
  - Mozilla Firefox: Nhấn tổ hợp phím Ctrl + Shift + Del. Chọn các mục như dưới đây và nhấn OK.



- Google Chrome: Nhấn tổ hợp phím Ctrl + Shift + Del. Chọn the past day. Chọn Cached images and files. Nhấp nút Clear data.



- **Bước 5:** Trên cửa sổ Command Prompt, thực hiện lệnh ipconfig /flushdns
- **Bước 6:** Khởi động phần mềm Wireshark và chọn bắt gói tin trên các mạng phù hợp
- **Bước 7:** Quay trở lại cửa sổ trình duyệt, upload file alice.txt đã download ở bước số 2

### Upload page for TCP Wireshark Lab

Computer Networking: A Top Down Approach, 6th edition  
Copyright 2012 J.F. Kurose and K.W. Ross, All Rights Reserved

If you have followed the instructions for the TCP Wireshark Lab, you have *already* downloaded an ASCII copy of alice from <http://nct.soict.hust.edu.vn/mmt/alice.txt> and you also *already* have the Wireshark packet sniffer running and capturing packets on your computer.

Click on the Browse button below to select the directory/file name for the copy of alice.txt that is stored on your computer.

alice.txt 1

Once you have selected the file, click on the "Upload alice.txt file" button below. This will cause your browser to send a copy of alice.txt over an HTTP connection (using TCP) to the web server at nct.soict.hust.edu.vn. After clicking on the button, wait until a short message is displayed indicating the the upload is complete. Then stop your Wireshark packet sniffer - you're ready to begin analyzing the TCP transfer of alice.txt from your computer to nct.soict.hust.edu.vn!!

2

- **Bước 8:** Sau khi thông báo hiển thị upload file thành công xuất hiện, đợi thêm khoảng 30 giây và dừng bắt gói tin trên Wireshark. Hình ảnh lưu lượng bắt được trên Wireshark có một phần tương tự như hình ảnh sau:

2 0.839954	192.168.1.176	8.8.8.8	DNS	81 Standard query 0x1c59 A nct.soict.hust.edu.vn
3 0.906865	8.8.8.8	192.168.1.176	DNS	97 Standard query response 0x1c59 A nct.soict.hust.edu.vn A 202.191.56.66
4 0.908215	192.168.1.176	202.191.56.66	TCP	66 5729 → 80 [SYN] Seq=2221575575 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5 0.908536	192.168.1.176	8.8.8.8	DNS	81 Standard query 0x6d03 A nct.soict.hust.edu.vn
6 0.910222	202.191.56.66	192.168.1.176	TCP	66 80 → 5729 [SYN, ACK] Seq=943466327 Ack=2221575576 Win=29200 Len=0 MSS=1460
7 0.910378	192.168.1.176	202.191.56.66	TCP	54 5729 → 80 [ACK] Seq=2221575576 Ack=943466328 Win=131328 Len=0
8 0.913761	192.168.1.176	202.191.56.66	TCP	1514 5729 → 80 [ACK] Seq=2221575576 Ack=943466328 Win=131328 Len=1460
9 0.913761	192.168.1.176	202.191.56.66	TCP	1514 5729 → 80 [ACK] Seq=2221577036 Ack=943466328 Win=131328 Len=1460
10 0.913764	192.168.1.176	202.191.56.66	TCP	1514 5729 → 80 [ACK] Seq=2221578496 Ack=943466328 Win=131328 Len=1460
11 0.913764	192.168.1.176	202.191.56.66	TCP	1514 5729 → 80 [ACK] Seq=2221579956 Ack=943466328 Win=131328 Len=1460
12 0.913764	192.168.1.176	202.191.56.66	TCP	1514 5729 → 80 [ACK] Seq=2221581416 Ack=943466328 Win=131328 Len=1460
13 0.913765	192.168.1.176	202.191.56.66	TCP	946 5729 → 80 [PSH, ACK] Seq=2221582876 Ack=943466328 Win=131328 Len=892
14 0.913936	192.168.1.176	202.191.56.66	TCP	1514 5729 → 80 [ACK] Seq=2221583768 Ack=943466328 Win=131328 Len=1460

#### Lưu ý:

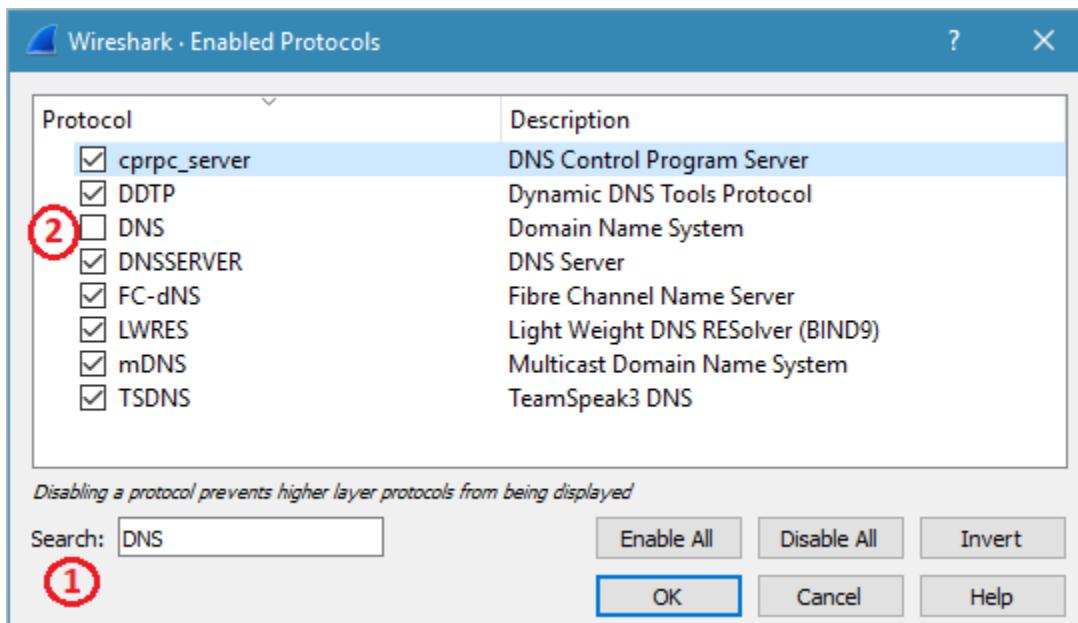
- Nếu file lưu lượng trên máy sinh viên không có các gói tin có Protocol là DNS thì thực hiện lại từ bước 3.
- Các gói tin bắt được trên máy sinh viên có thể sẽ có một số thông số khác với hình ảnh minh họa. Điều này là hoàn toàn bình thường và không có ảnh hưởng tới quá trình thực hành

- **Bước 9:** Lưu file lưu lượng có tên là **lab04.pcapng** và nộp cùng báo cáo thực hành

### 6.2.3. Quan sát các gói tin UDP

Sử dụng file lưu lượng ở mục 3.2 để quan sát và trả lời các câu hỏi.

- **Bước 1:** Trên menu của Wireshark, chọn **Analyze → Enabled Protocols**. Điền DNS vào ô **Search** và bỏ chọn mục DNS trong danh sách Protocol như hình dưới đây sau. Nhấn OK để đóng cửa sổ.



- **Bước 2:** Điền giá trị **udp** vào mục Filter của Wireshark để lọc ra các gói tin UDP đã bắt được tương tự như hình minh họa dưới đây.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.839954	192.168.1.176	8.8.8.8	UDP	81	55309 → 53 Len=39
3	0.906865	8.8.8.8	192.168.1.176	UDP	97	53 → 55309 Len=55
5	0.908536	192.168.1.176	8.8.8.8	UDP	81	54722 → 53 Len=39
92	0.956218	8.8.8.8	192.168.1.176	UDP	97	53 → 54722 Len=55
139	0.957318	192.168.1.176	8.8.8.8	UDP	81	52525 → 53 Len=39
163	1.040953	8.8.8.8	192.168.1.176	UDP	132	53 → 52525 Len=90
169	3.993781	192.168.1.144	192.168.1.255	UDP	85	5050 → 5050 Len=43

- **Bước 3:** Chọn một gói tin UDP được gửi đi từ máy của sinh viên và trả lời câu hỏi 1.

**Câu hỏi 1(1 điểm):** Xác định các thông số sau của gói tin.STT gói tin(No.):.....

Địa chỉ IP nguồn: ..... Địa chỉ IP đích: .....

Số hiệu cổng nguồn: ..... Số hiệu cổng đích: .....

Gói tin này được đóng gói vào gói tin của giao thức tầng mạng nào?

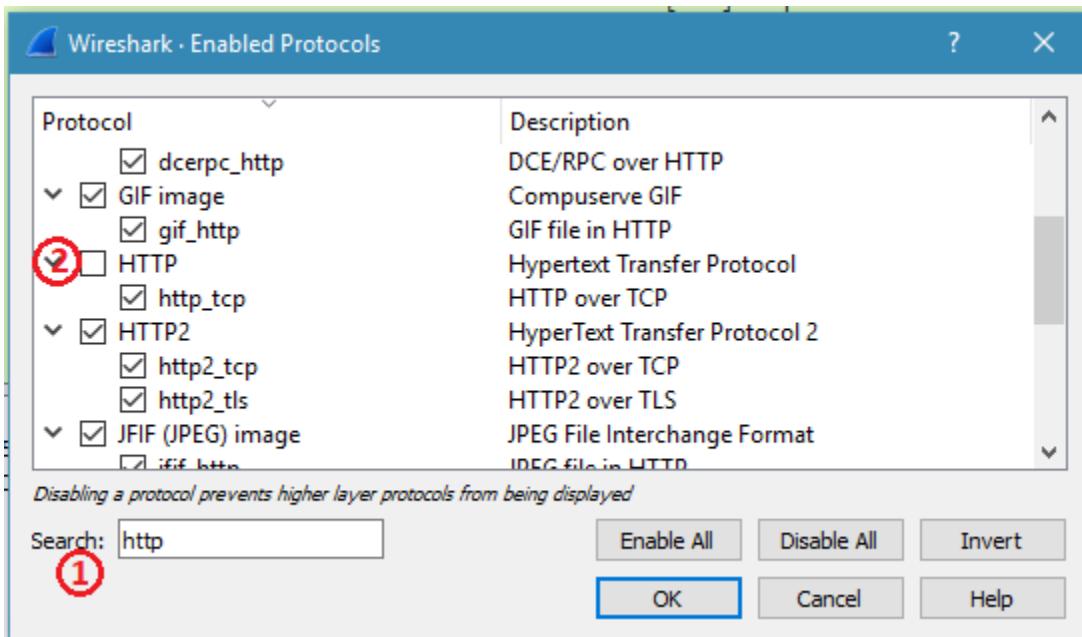
- **Bước 4:** Tìm gói tin mà máy đích trả lời cho gói tin ở bước 3 và trả lời câu hỏi 2.

**Câu hỏi 2(1 điểm):** STT gói tin:.... Tại sao xác định được đây là gói tin trả lời cho gói tin ở bước 3? Máy đích có thể biết được gói tin này đã được truyền thành công hay không? Tại sao?

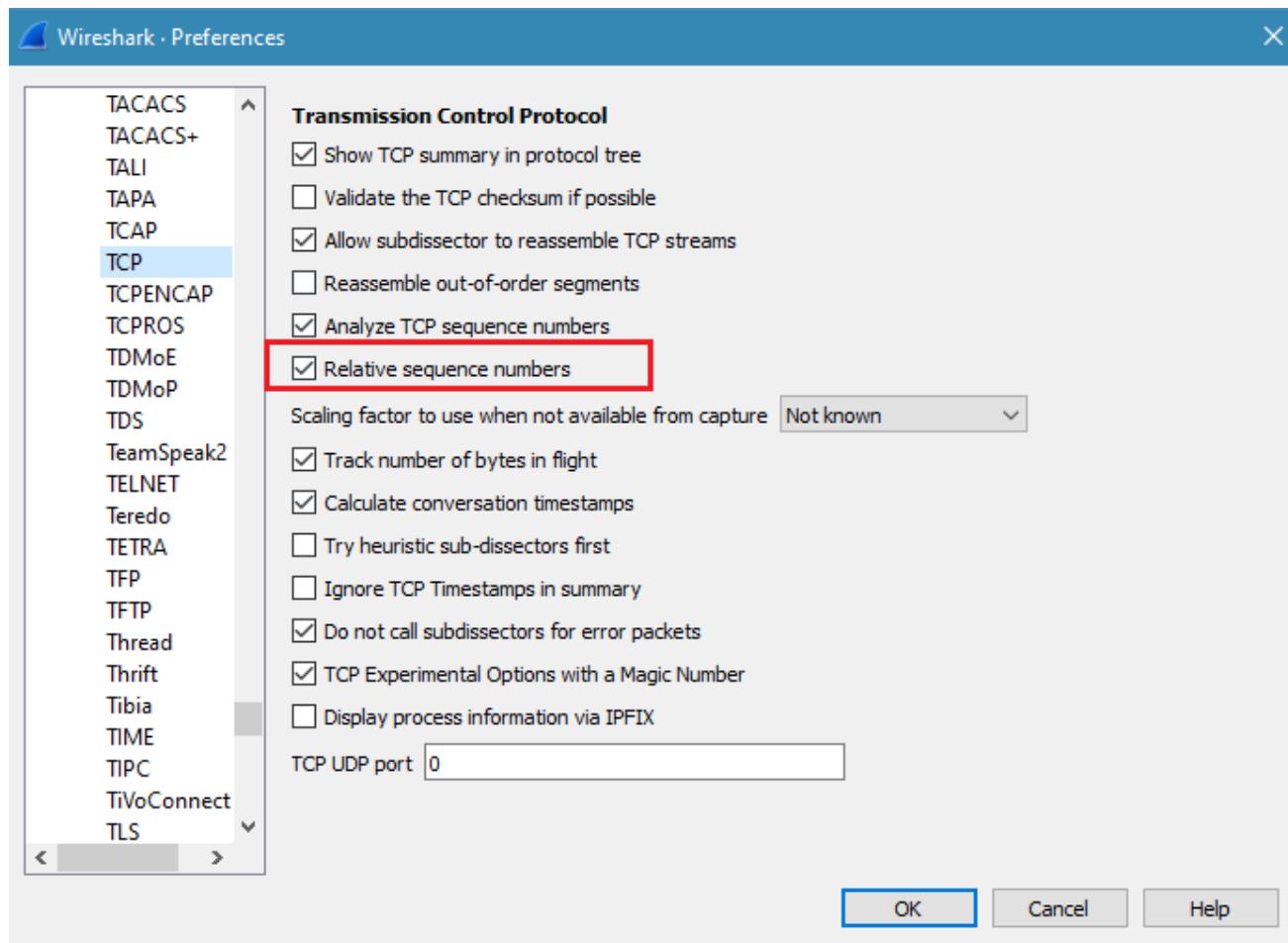
#### 6.2.4. Quan sát các gói tin TCP

Sử dụng file lưu lượng ở mục 3.2 để quan sát và trả lời các câu hỏi.

- **Bước 1:** Trên menu của Wireshark, chọn **Analyze → Enabled Protocols**. Điền HTTP vào ô **Search** và bỏ chọn mục HTTP trong danh sách Protocol như hình dưới đây sau. Nhấn OK để đóng cửa sổ.



Trên menu của Wireshark, chọn **Edit → Preferences...** Trong mục **Protocol** của cửa sổ **Preference**, chọn **TCP**. Nhấn chọn mục **Relative sequence numbers** như hình sau:



- **Bước 2:** Điền giá trị sau vào mục Filter của Wireshark để lọc ra các gói tin TCP đã bắt được trong quá trình upload file.

**tcp && ip.addr == 202.191.56.66**

Hình dưới đây minh họa kết quả thực hiện:

tcp && ip.addr == 202.191.56.66						
No.	Time	Source	Destination	Protocol	Length	Info
4	0.908215	192.168.1.176	202.191.56.66	TCP	66	5729 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 S
6	0.910222	202.191.56.66	192.168.1.176	TCP	66	80 → 5729 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=14
7	0.910378	192.168.1.176	202.191.56.66	TCP	54	5729 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
8	0.913761	192.168.1.176	202.191.56.66	TCP	1514	5729 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=1460
9	0.913761	192.168.1.176	202.191.56.66	TCP	1514	5729 → 80 [ACK] Seq=1461 Ack=1 Win=131328 Len=1460
10	0.913764	192.168.1.176	202.191.56.66	TCP	1514	5729 → 80 [ACK] Seq=2921 Ack=1 Win=131328 Len=1460
11	0.913764	192.168.1.176	202.191.56.66	TCP	1514	5729 → 80 [ACK] Seq=4381 Ack=1 Win=131328 Len=1460
12	0.913764	192.168.1.176	202.191.56.66	TCP	1514	5729 → 80 [ACK] Seq=5841 Ack=1 Win=131328 Len=1460
13	0.913765	192.168.1.176	202.191.56.66	TCP	946	5729 → 80 [PSH, ACK] Seq=7301 Ack=1 Win=131328 Len=892
14	0.913936	192.168.1.176	202.191.56.66	TCP	1514	5729 → 80 [ACK] Seq=8193 Ack=1 Win=131328 Len=1460
15	0.913937	192.168.1.176	202.191.56.66	TCP	1514	5729 → 80 [ACK] Seq=9653 Ack=1 Win=131328 Len=1460
16	0.913937	192.168.1.176	202.191.56.66	TCP	1514	5729 → 80 [ACK] Seq=11113 Ack=1 Win=131328 Len=1460

- **Bước 3:** Tìm các gói tin được sử dụng để thiết lập liên kết giữa tiến trình Web Browser trên máy tính của sinh viên và máy chủ Web trong quá trình truy cập. Trả lời câu hỏi số 3

**Câu hỏi 3(2 điểm):** Địa chỉ của các bên trong liên kết là gì?

Địa chỉ IP bên khởi tạo ..... Địa chỉ IP bên đáp ứng:.....

Số hiệu cổng ứng dụng bên khởi tạo:.....

Số hiệu cổng ứng dụng bên đáp ứng:.....

Với mỗi gói tin trong quá trình thiết lập liên kết, hãy cho biết các thông số sau:

STT gói tin (No.)	Giá trị <b>nhị phân</b> của trường Flags	Các cờ được thiết lập	Sequence number	ACK number	Kích thước phần dữ liệu

- **Bước 4:** Tìm gói tin đầu tiên có chứa dữ liệu của file alice.txt đã upload và trả lời câu hỏi số 4. (Gợi ý: Xem nội dung phần payload và so sánh với nội dung phần đầu file alice.txt)

**Câu hỏi 4(1 điểm):** Xác định các thông số sau của gói tin

- STT gói tin (No.):
- Địa chỉ IP nguồn:
- Địa chỉ IP đích:
- Số hiệu cổng nguồn:
- Số hiệu cổng đích:
- Sequence Number:
- ACK Number:
- Kích thước phần tiêu đề TCP:
- Kích thước phần dữ liệu:
- Các cờ được thiết lập:
- Gói tin này được đóng gói vào gói tin của giao thức tầng mạng nào?

Hãy để ý rằng các thông số địa chỉ trên gói tin này có phù hợp với các thông số địa chỉ trong quá trình thiết lập liên kết hay không?

- **Bước 5:** Tìm gói tin báo nhận của Web Server cho gói tin đã quan sát ở bước 4 và trả lời câu hỏi số 5 và số 6.

**Câu hỏi 5(1 điểm):** Xác định các thông số sau của gói tin

- *STT gói tin (No.):*
- *Địa chỉ IP nguồn:*
- *Địa chỉ IP đích:*
- *Số hiệu cổng nguồn:*
- *Số hiệu cổng đích:*
- *Sequence Number:*
- *ACK Number:*
- *Kích thước phần tiêu đề TCP:*
- *Kích thước phần dữ liệu:*
- *Các cờ được thiết lập:*

Có thể kết luận chắc chắn Web Server đã nhận thành công gói tin ở bước 4 hay không?  
Tại sao?

**Câu hỏi 6(1 điểm):** Gói tin tiếp theo chứa dữ liệu của file được Web Browser gửi đi có giá trị Sequence Number là bao nhiêu?

Lưu ý: Kích thước phần dữ liệu trong gói tin quan sát được ở bước 4 có thể lớn hơn giá trị Maximum Segment Size theo lý thuyết của giao thức TCP. Đó là do hệ điều hành kích hoạt cơ chế TCP Large Segment Offload.

- **Bước 6:** Tìm các gói tin được sử dụng để đóng liên kết TCP đã thiết lập và trả lời câu hỏi số 7.

Lưu ý: Nếu không tìm thấy đầy đủ các gói tin TCP để đóng liên kết, có thể trình duyệt duy trì liên kết lâu hơn. Sinh viên nên thực hiện lại thao tác bắt gói tin của mục 3.2 và chờ khoảng thời gian lâu hơn trong bước 8.

**Câu hỏi 7(2 điểm):** Với mỗi gói tin trong quá trình đóng liên kết, hãy cho biết các thông số sau:

<i>STT gói tin (No.)</i>	<i>Giá trị nhị phân của trường Flags</i>	<i>Các cờ được thiết lập</i>	<i>Sequence number</i>	<i>ACK number</i>	<i>Kích thước phần dữ liệu</i>	
<b>Câu hỏi 8(1 điểm):</b> Tính thông lượng trung bình trên liên kết TCP trong quá trình upload file lên máy chủ.						

### **3. BÀI THỰC HÀNH SỐ 5: PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC DNS VÀ HTTP**

#### **7.1. MỤC ĐÍCH VÀ NỘI DUNG**

##### **7.1.1. Mục đích**

Bài thí nghiệm này được thiết kế để trang bị cho sinh viên các kỹ năng sử dụng phần mềm Wireshark để bắt và lọc các gói tin DNS, HTTP theo yêu cầu. Thông qua đó, sinh viên có thể quan sát và hiểu được các hoạt động quan trọng của hai giao thức này. Bên cạnh đó, thông qua việc vận dụng kiến thức lý thuyết, sinh viên có thể giải thích kết quả đã quan sát được.

##### **7.1.2. Yêu cầu đối với sinh viên**

- Môi trường thực hành:
  - Sử dụng thành thạo các chức năng cơ bản của phần mềm Wireshark
  - Thực hiện thành thạo các thao tác trên hệ điều hành Windows, bao gồm các thao tác với thông số TCP/IP đã được hướng dẫn trong các bài thực hành trước.
- Kiến thức: Nắm vững kiến thức về tầng ứng dụng, các giao thức DNS và HTTP.
- Viết báo cáo thực hành và nộp kết quả theo yêu cầu như sau:
  - Báo cáo(bản giấy) theo mẫu đã cung cấp
  - File lưu lượng lab05.pcapng đặt trong thư mục có tên định dạng **TenSV\_MSSV\_Lab05**. Nén thư mục và gửi vào địa chỉ email theo yêu cầu của cán bộ hướng dẫn thực hành.

### **7.1.3. Cơ sở lý thuyết**

#### **7.1.3.1. Tên miền và hệ thống DNS**

Tên miền là một chuỗi ký tự định danh cho nút mạng, bao gồm các nhãn (label) cách nhau bởi dấu '.', ví dụ soict.hust.edu.vn là tên miền cho máy chủ Web của Viện CNTT-TT, Đại học Bách khoa Hà Nội. Đối với người dùng, thay vì phải nhớ địa chỉ IP là các giá trị số khó nhớ, người dùng có thể truy cập vào dịch vụ bằng tên miền của máy chủ. Tuy nhiên, trong quá trình truyền tin, các nút mạng lại sử dụng địa chỉ IP. Do đó, tên miền cần phải được ánh xạ tới một hoặc nhiều địa chỉ IP nào đó. Trên mạng Internet, tên miền và ánh xạ này, cùng với các thông tin khác, được quản lý bởi các máy chủ trong hệ thống tên miền DNS. Bên cạnh đó, các máy chủ DNS này cung cấp dịch vụ tìm kiếm thông tin tên miền. Khi một nút mạng muốn gửi thông tin tới nút mạng khác mà chỉ biết tên miền, nó sẽ phải thực hiện quá trình tìm kiếm thông tin tên miền. Trong hầu hết các trường hợp, quá trình này bắt đầu bằng việc client gửi thông điệp DNS Query yêu cầu truy vấn tới máy chủ DNS. Kết quả tìm kiếm được đóng gói trong thông điệp DNS Response và trả lại cho client. Các bên trong dịch vụ DNS sử dụng giao thức UDP của tầng giao vận để truyền thông điệp với số hiệu cổng dịch vụ chuẩn trên máy chủ là 53.

#### **7.1.3.2. Dịch vụ Web và giao thức HTTP**

World Wide Web, gọi tắt là Web, lần đầu tiên được giới thiệu bởi Tim Berners-Lee vào năm 1991 với ý tưởng chính là liên kết các thông tin trên mạng Internet qua địa chỉ URL (Uniform Resource Location) và trình bày thành một văn bản sử dụng mã HTML (Hyper Text Markup Language) gọi là Webpage. Tập hợp các Webpage được lưu trữ trên một máy chủ Web để tạo thành một Website. Người dùng có thể dễ dàng sử dụng trình duyệt Web như là một phần mềm client để truy cập vào Website. Mặc dù là dịch vụ ra đời muộn hơn so với các dịch vụ truyền thống khác trên Internet, như là email hay truyền file, nhưng nhờ sự dễ dàng trong việc liên kết và chia sẻ thông tin mà Web đã nhanh chóng phổ biến và phát triển với tốc độ chóng mặt. Cho đến ngày nay, Web vừa là dịch vụ phổ biến nhất trên mạng Internet, vừa là một nền tảng để phát triển các dịch vụ khác.

Giao thức HTTP được Tim Berners-Lee phát triển để điều khiển hoạt động của dịch vụ Web. So với phiên bản HTTP 0.9 và HTTP 1.0 ở giai đoạn trước, phiên bản HTTP 1.1 hiện nay đã có nhiều cải tiến để nâng cao hiệu năng hoạt động của dịch vụ. Tuy nhiên, các nguyên lý cơ bản trong hoạt động vẫn được giữ nguyên. HTTP là một giao thức hướng liên kết, trong đó nó sử dụng dịch vụ của giao thức TCP trên tầng giao vận để thiết lập liên kết và điều khiển truyền các thông điệp HTTP trên liên kết đó. Máy chủ

Web sử dụng cổng dịch vụ có số hiệu 80 để lắng nghe các yêu cầu thiết lập liên kết được gửi tới từ client. Để yêu cầu nội dung của Website, client gửi đi thông điệp HTTP Request và chờ nhận thông điệp HTTP Response trả lời. Hiện nay, do các vấn đề về bảo mật, giao thức HTTPS dần được thay thế để đảm bảo an toàn cho quá trình truyền tin trong dịch vụ Web. HTTPS là cải tiến của HTTP, trong đó liên kết SSL/TLS được sử dụng thay cho liên kết TCP và số hiệu cổng ứng dụng là 443. Trên liên kết SSL/TLS, các thông điệp HTTP sẽ được mã hóa nhằm bảo vệ tính bí mật, toàn vẹn cho dữ liệu.

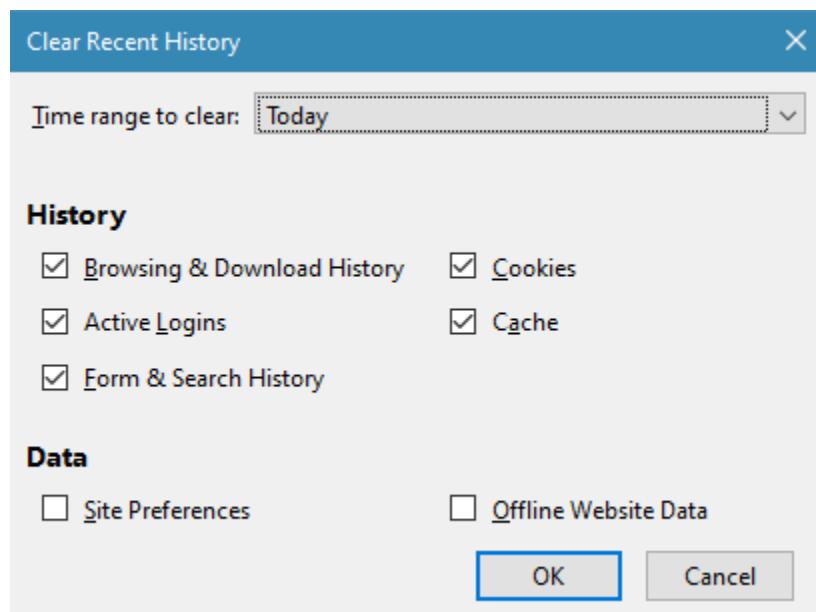
## 7.2. NỘI DUNG THỰC HÀNH

### 7.2.1. Xác định thông số của máy trạm

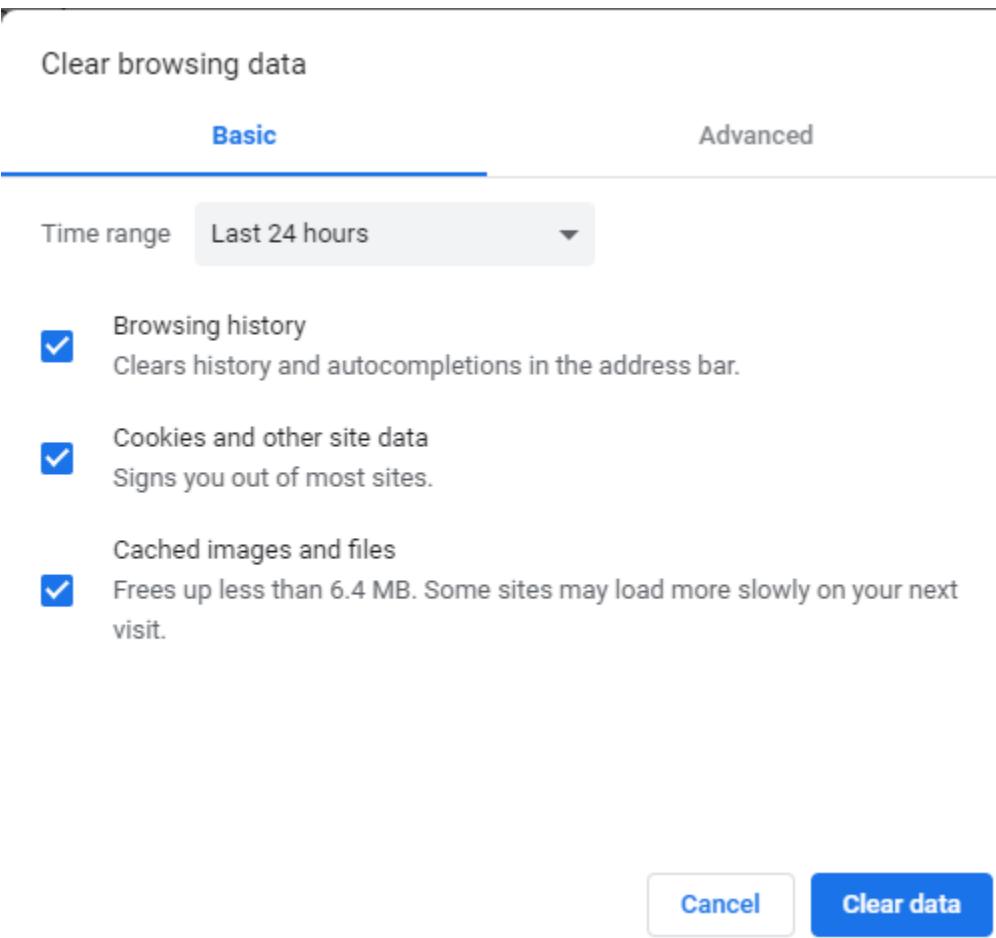
Sinh viên xác định địa chỉ IP, địa chỉ DNS Server trên máy tính ở phòng thực hành và ghi vào báo cáo. Để có được thông tin này, sinh viên xem lại bài thực hành số 2 và 3.

### 7.2.2. Thu thập lưu lượng mạng

- **Bước 1:** Tắt các chương trình của người dùng có trao đổi dữ liệu trên mạng trừ trình duyệt Web.
- **Bước 2:** Xóa bộ đệm của trình duyệt
  - Mozilla Firefox: Nhấn tổ hợp phím Ctrl + Shift + Del. Chọn các mục như dưới đây và nhấn OK.



- Google Chrome: Nhấn tổ hợp phím Ctrl + Shift + Del. Chọn the past day. Chọn Cached images and files. Nhấn nút Clear data.



- **Bước 3:** Trên cửa sổ Command Prompt, thực hiện lệnh ipconfig /flushdns
- **Bước 4:** Khởi động phần mềm Wireshark và chọn bắt gói tin trên các mạng phù hợp
- **Bước 5:** Trên trình duyệt Web, mở cửa sổ duyệt riêng tư (Private Browsing):
  - **Mozilla Firefox:** Nhấn tổ hợp phím Ctrl + Shift + P
  - **Google Chrome:** Nhấn tổ hợp phím Ctrl + Shift + N

Truy cập vào địa chỉ sau:

<http://nct.soict.hust.edu.vn/mmt/lab05/>

Lưu ý: Các bước trên có tác dụng giúp ta quan sát đầy đủ hơn hoạt động của các dịch vụ.

- **Bước 6:** Sau khi trình duyệt đã tải xong trang Web khoảng 5-10 giây, dừng việc bắt gói tin trên Wireshark. Hình ảnh lưu lượng bắt được trên Wireshark có thể như sau:

No.	Time	Source	Destination	Protocol	Length	Info
25	4.682835	192.168.1.176	8.8.8.8	DNS	81	Standard query 0x54e1 A nct.soi.ct.hust.edu.vn
26	4.751908	8.8.8.8	192.168.1.176	DNS	97	Standard query response 0x54e1 A nct.soi.ct.hust.edu.vn A 202.191.56.66
27	4.753094	192.168.1.176	202.191.56.66	TCP	66	7253 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
28	4.753348	192.168.1.176	8.8.8.8	DNS	81	Standard query 0xc89a A nct.soi.ct.hust.edu.vn
29	4.755770	202.191.56.66	192.168.1.176	TCP	66	80 → 7253 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
30	4.755870	192.168.1.176	202.191.56.66	TCP	54	7253 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
31	4.757913	192.168.1.176	202.191.56.66	HTTP	414	GET /mmt/lab05/ HTTP/1.1
32	4.760169	202.191.56.66	192.168.1.176	TCP	60	80 → 7253 [ACK] Seq=1 Ack=361 Win=30336 Len=0
33	4.761982	202.191.56.66	192.168.1.176	TCP	1514	80 → 7253 [ACK] Seq=1 Ack=361 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
34	4.763646	202.191.56.66	192.168.1.176	TCP	1514	80 → 7253 [ACK] Seq=1461 Ack=361 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
35	4.763687	192.168.1.176	202.191.56.66	TCP	54	7253 → 80 [ACK] Seq=361 Ack=2921 Win=131328 Len=0
36	4.764615	202.191.56.66	192.168.1.176	TCP	1514	80 → 7253 [ACK] Seq=2921 Ack=361 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
37	4.765585	202.191.56.66	192.168.1.176	TCP	1514	80 → 7253 [ACK] Seq=4381 Ack=361 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
38	4.765622	192.168.1.176	202.191.56.66	TCP	54	7253 → 80 [ACK] Seq=361 Ack=5841 Win=131328 Len=0
39	4.766565	202.191.56.66	192.168.1.176	TCP	1514	80 → 7253 [ACK] Seq=5841 Ack=361 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
40	4.766913	202.191.56.66	192.168.1.176	TCP	1514	80 → 7253 [ACK] Seq=7301 Ack=361 Win=30336 Len=1460 [TCP segment of a reassembled PDU]

### Lưu ý:

- Trên menu của Wireshark chọn Analyze → Enabled Protocols. Kiểm tra để chắc chắn các mục DNS, HTTP đã được chọn.
- Nếu file lưu lượng trên máy sinh viên không có các gói tin có Protocol là DNS thì thực hiện lại từ bước 2.
- Các gói tin bắt được trên máy sinh viên có thể sẽ có một số thông số khác với hình ảnh minh họa. Điều này là hoàn toàn bình thường và không có ảnh hưởng tới quá trình thực hành
- **Bước 7:** Lưu file lưu lượng có tên là **lab05.pcapng** và nộp cùng báo cáo thực hành

### 7.2.3. Quan sát quá trình truyền dữ liệu trong DNS

Sử dụng file lưu lượng ở mục 3.2 để quan sát và trả lời các câu hỏi.

- **Bước 1:** Điền giá trị **dns** vào mục Filter của Wireshark để lọc ra các thông điệp DNS đã bắt được tương tự như hình minh họa dưới đây.

No.	Time	Source	Destination	Protocol	Length	Info
25	4.682835	192.168.1.176	8.8.8.8	DNS	81	Standard query 0x54e1 A nct.soi.ct.hust.edu.vn
26	4.751908	8.8.8.8	192.168.1.176	DNS	97	Standard query response 0x54e1 A nct.soi.ct.hust.edu.vn A 202.191.56.66
28	4.753348	192.168.1.176	8.8.8.8	DNS	81	Standard query 0xc89a A nct.soi.ct.hust.edu.vn
57	4.808481	192.168.1.176	8.8.8.8	DNS	92	Standard query 0x175e AAAA ff.kis.v2.scr.kaspersky-labs.com
60	4.810552	192.168.1.176	8.8.8.8	DNS	84	Standard query 0x35f4 A www.lingosolutions.co.uk
95	4.830542	8.8.8.8	192.168.1.176	DNS	97	Standard query response 0xc89a A nct.soi.ct.hust.edu.vn A 202.191.56.66
96	4.831702	192.168.1.176	8.8.8.8	DNS	81	Standard query 0x3221 AAAA nct.soi.ct.hust.edu.vn
100	4.832592	8.8.8.8	192.168.1.176	DNS	174	Standard query response 0x175e AAAA ff.kis.v2.scr.kaspersky-labs.com SOA d
276	4.937883	8.8.8.8	192.168.1.176	DNS	132	Standard query response 0x3221 AAAA nct.soi.ct.hust.edu.vn SOA dns.hust.edu
280	5.131132	8.8.8.8	192.168.1.176	DNS	100	Standard query response 0x35f4 A www.lingosolutions.co.uk A 149.255.58.41
282	5.133981	192.168.1.176	8.8.8.8	DNS	84	Standard query 0x8645 A www.lingosolutions.co.uk
286	5.425351	8.8.8.8	192.168.1.176	DNS	100	Standard query response 0x8645 A www.lingosolutions.co.uk A 149.255.58.41
287	5.427220	192.168.1.176	8.8.8.8	DNS	84	Standard query 0xe374 AAAA www.lingosolutions.co.uk
305	5.731849	8.8.8.8	192.168.1.176	DNS	147	Standard query response 0xe374 AAAA www.lingosolutions.co.uk SOA ns1.unlim

- **Bước 2:** Chọn gói tin DNS được trình duyệt gửi đi để yêu cầu phân giải tên miền của Website đã truy cập và trả lời câu hỏi 1.

Lưu ý: Nếu không tìm thấy gói tin nào, sinh viên cần thực hiện lại các thao tác của mục 3.2.

**Câu hỏi 1(1 điểm):** Hãy xác định các thông tin sau trên thông điệp

- *STT gói tin(No.):*
- *Giao thức tầng giao vận được sử dụng để gửi thông điệp đi:*
- *Địa chỉ IP nguồn:*
- *Số hiệu cổng ứng dụng nguồn:*
- *Địa chỉ IP đích:*
- *Số hiệu cổng đích? Đây là số hiệu cổng ứng dụng của dịch vụ nào?*
- *Kiểu thông tin truy vấn(Type):*

Qua việc xác định các thông số mạng trên máy trạm của sinh viên ở mục 3.1, cho biết thông điệp này được gửi tới nút mạng nào?

- **Bước 3:** Tìm thông điệp DNS Response trả lời cho thông điệp yêu cầu ở bước 2 để quan sát và trả lời câu hỏi 2

**Câu hỏi 2(1 điểm):** Hãy xác định các thông tin sau trên thông điệp

- *STT gói tin(No.):*
- *Giao thức tầng giao vận được sử dụng để gửi thông điệp đi:*
- *Địa chỉ IP nguồn:*
- *Số hiệu cổng ứng dụng nguồn:*
- *Địa chỉ IP đích:*
- *Số hiệu cổng đích:*
- *Kiểu thông tin truy vấn(Type):*
- *Tên miền được truy vấn:*
- *Địa chỉ IP của tên miền được truy vấn:*

Tại sao xác định được đây là thông điệp trả lời cho thông điệp yêu cầu ở bước 2?

- **Bước 4:** Quan sát tất cả các thông điệp DNS và trả lời câu hỏi 3?

**Câu hỏi 3(1 điểm):** Tại sao ngoài tên miền nct.soict.hust.edu.vn được truy vấn do người dùng truy cập vào trang Web <http://nct.soict.hust.edu.vn/mmt/lab05/>, còn có truy vấn tới tên miền khác. Các tên miền khác được truy vấn và địa chỉ IP của các tên miền đó là gì?

#### 7.2.4. Quan sát quá trình truyền dữ liệu của HTTP

Sử dụng file lưu lượng ở mục 3.2 để quan sát và trả lời các câu hỏi.

- **Bước 1:** Giả sử ở phần trên, sinh viên đã quan sát được địa chỉ IP phân giải từ tên miền nct.soict.hust.edu.vn của máy chủ Web là X. Điền giá trị **ip.addr == X** (*Lưu ý: Thay X bằng địa chỉ IP đã quan sát được*) vào mục Filter của Wireshark. Sinh viên sẽ quan sát thấy các thông điệp mà máy trạm trao đổi với máy chủ Web.

**Câu hỏi 4(1 điểm):** Trước khi thông điệp HTTP đầu tiên được gửi đi tới máy chủ nct.soict.hust.edu.vn, máy trạm và máy chủ đã thực hiện quá trình gì? Số thứ tự (No) của các gói tin trong quá trình đó mà sinh viên quan sát được là gì? Số hiệu cổng ứng dụng của các bên đã sử dụng là bao nhiêu? Số hiệu cổng ứng dụng trên máy chủ là cổng ứng dụng của dịch vụ nào?

- **Bước 2:** Điền giá trị **http** vào mục Filter của Wireshark. Sinh viên sẽ quan sát thấy các gói tin HTTP mà máy trạm đã trao đổi trên mạng.
- **Bước 3:** Quan sát các thông điệp HTTP trao đổi giữa máy trạm và máy chủ Web nct.soict.hust.edu.vn và trả lời câu hỏi 5

**Câu hỏi 5(2 điểm):** Có bao nhiêu thông điệp HTTP Request được gửi đi? Liệt kê các thông tin sau về các thông điệp HTTP giữa máy trạm và máy chủ Web nct.soict.hust.edu.vn

HTTP Request			HTTP Response		
No.	Phương thức yêu cầu	Đối tượng yêu cầu	No.	Mã trả lời	Ý nghĩa mã trả lời

Trong các thông điệp HTTP Request, có những thông điệp nào được gửi đi liên tiếp mà không đợi thông điệp trả lời từ máy chủ không? Nếu có, tại sao trình duyệt Web trên máy trạm thực hiện như vậy?

- **Bước 4:** Chọn thông điệp HTTP Request đầu tiên được máy trạm gửi cho máy chủ Web nct.hust.edu.vn và trả lời câu hỏi 6.

**Câu hỏi 6(1 điểm):** Hãy cho biết các thông tin sau về thông điệp yêu cầu:

- *Giao thức tầng giao vận được sử dụng để truyền thông điệp*

- Số hiệu cổng ứng dụng đích
- Phiên bản của giao thức HTTP mà máy trạm sử dụng
- Giá trị của trường Connection trong tiêu đề HTTP

- **Bước 5:** Tìm thông điệp HTTP Response mà máy chủ Web trả lời cho thông điệp yêu cầu ở bước 5 và trả lời câu hỏi 7

**Câu hỏi 7(1 điểm):** Hãy cho biết các thông tin sau về thông điệp trả lời:

- Phiên bản của giao thức HTTP mà máy chủ sử dụng
- Giá trị của trường Connection trong tiêu đề HTTP
- Phần thân chứa dữ liệu gì? Dữ liệu này có kích thước là bao nhiêu?
- Thông điệp này đóng gói trong bao nhiêu gói tin TCP?

Sau khi thông điệp này được gửi đi, kết nối TCP còn được duy trì không?

**Câu hỏi 8(1 điểm):** Ngoài quá trình trao đổi dữ liệu với máy chủ Web nct.soict.hust.edu.vn, máy trạm còn gửi thông điệp HTTP Request tới máy chủ Web có tên miền và địa chỉ IP là gì? Tại sao máy trạm phát đi thông điệp này? (Gợi ý: Xem lại nội dung trong phần thân của thông điệp HTTP Response trong bước 5)

Xem phần tiêu đề của thông điệp HTTP Request trên và cho biết giá trị trường Referer là gì?

**Câu hỏi 9(1 điểm):** Đoạn sau đây mô tả ngắn gọn quá trình xử lý truy cập vào một trang Web trên trình duyệt Web. Hãy điền vào chỗ trống cụm từ còn thiếu

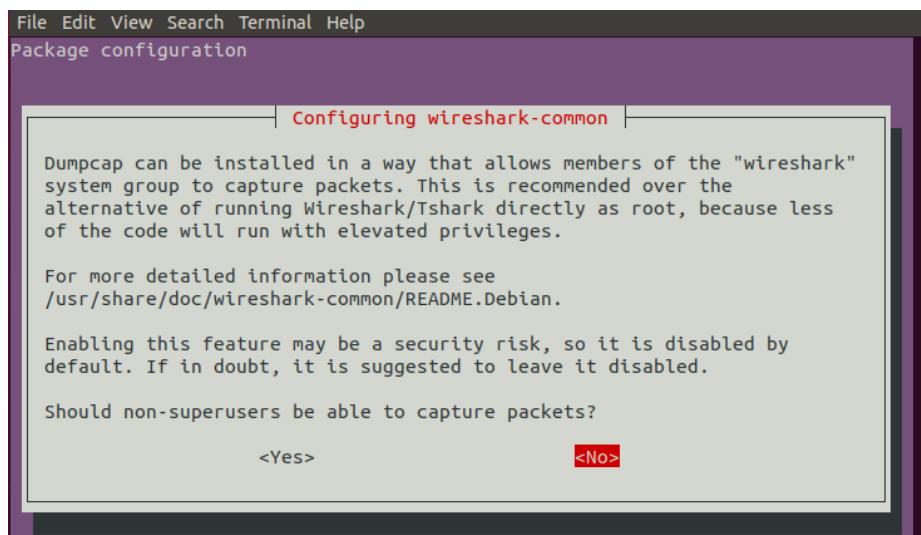
Khi nhận được yêu cầu truy cập vào một trang Web nào đó qua địa chỉ URL, nếu chưa biết địa chỉ IP của máy chủ Web. Trình duyệt gửi thông điệp .....tới ..... Trong thông điệp ..... trả lời nhận được, trình duyệt xác định được địa chỉ IP của máy chủ Web. Sau đó, trình duyệt gửi yêu cầu để thiết lập ..... với máy chủ Web. Trên .....đã được thiết lập, trình duyệt gửi đi thông điệp .....để yêu cầu nội dung của trang Web. Máy chủ Web tìm kiếm nội dung được yêu cầu và trả lại thông điệp ..... cùng với mã trả lời ..... nếu tìm thấy, hoặc mã ..... nếu không tìm thấy. Nếu hai bên sử dụng giao thức HTTP có phiên bản ..... thì liên kết sẽ được duy trì cho tới khi trình duyệt đã tải xong nội dung trang Web từ máy chủ.

## 4. PHỤ LỤC 1: LÀM QUEN VỚI CÔNG CỤ WIRESHAKR

### 8.1. Cài đặt Wireshark trên hệ điều hành Ubuntu 18.04

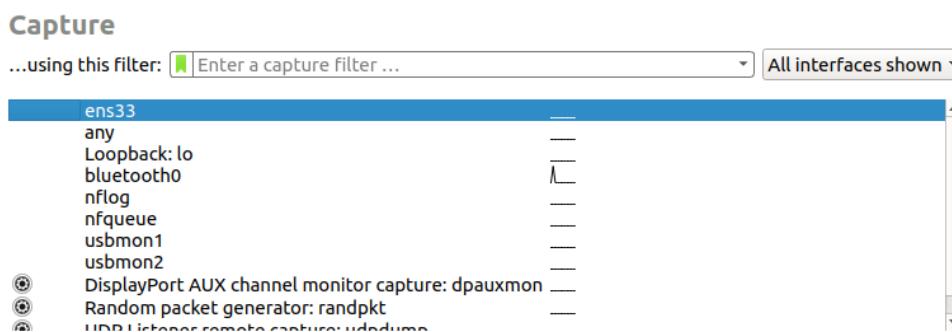
Wireshark là một công cụ kiểm tra, theo dõi và phân tích dữ liệu trao đổi giữa máy tính cài đặt công cụ này với các máy tính khác trong mạng. Sau đây, chúng ta sẽ cài đặt Wireshark trên hệ điều hành Ubuntu 18.04

Mở cửa sổ Terminal và thực hiện lệnh **sudo apt-get install wireshark -y** để cài đặt Wireshark. Trong quá trình cài đặt, chọn No khi gặp thông báo sau:



#### 8.1.1. Giao diện làm việc của Wireshark

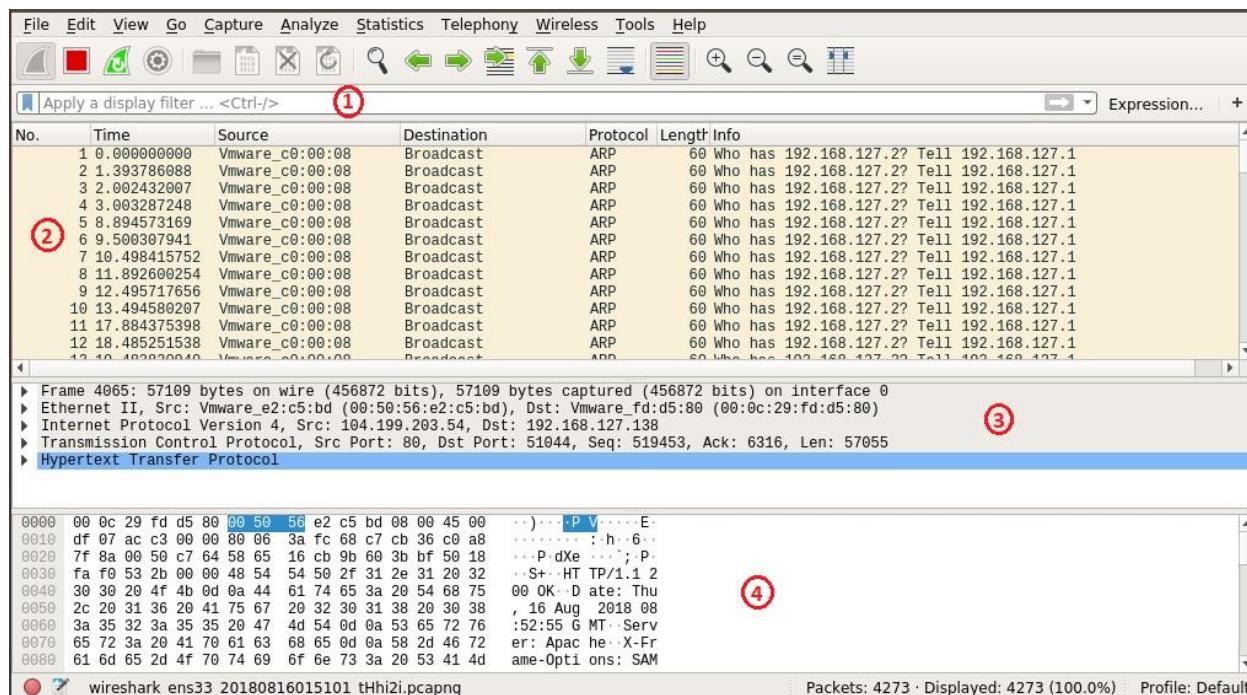
- Bước 1: Trên cửa sổ Terminal gõ lệnh **sudo wireshark** để khởi động phần mềm. Bỏ qua các cảnh báo nếu có.
- Bước 2: Sau khi Wireshark khởi động thành công, các bạn nhìn thấy danh sách các cổng giao tiếp khác nhau trên máy tính mà Wireshark có thể bắt các gói tin trên đó.



Lưu ý: Để biết các cổng mạng của máy tính, trên cửa sổ Terminal gõ lệnh **ip a**. Như kết quả hiển thị dưới đây, ta có thể thấy tên cổng mạng của máy tính là ens33

```
student@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:fd:d5:80 brd ff:ff:ff:ff:ff:ff
    inet 192.168.127.138/24 brd 192.168.127.255 scope global dynamic noprefixroute ens33
        valid_lft 955sec preferred_lft 955sec
    inet6 fe80::9608:58e8:2eba:a6a6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

- Bước 3: Nhấp đúp vào cổng mạng, chúng ta sẽ thấy giao diện làm việc của Wireshark như sau:



- Thanh công cụ : Xem mục **Help** của phần mềm để biết thêm chi tiết
- Vùng 1 : Tạo bộ lọc cho phép quan sát các gói tin thỏa mãn yêu cầu nào đó
- Vùng 2 : Danh sách các gói tin đã bắt.
  - ❖ **No.** : Số thứ tự gói tin
  - ❖ **Time** : thời điểm bắt (tính bằng giây kể từ khi bắt đầu)
  - ❖ **Source** : Địa chỉ nguồn của gói tin
  - ❖ **Destination** : Địa chỉ đích của gói tin
  - ❖ **Protocol** : Giao thức.

❖ **Length** : Kích thước

❖ **Info** : các thông tin chính về gói tin (thường lấy từ header của gói tin)

- Vùng 3 : Các nội dung phân tích được ở tất cả các tầng trong mô hình TCP/IP.
- Vùng 4 : Nội dung thực tế của gói tin

- Bước 4: Mở trình duyệt và truy cập vào trang <http://cyberlms.funix.edu.vn>

- Bước 5: Ngừng bắt gói tin bằng cách nhấp vào biểu tượng trên thanh công cụ. Chúng ta có thể lưu dữ liệu bắt được trên files có định dạng .pcapng

### 8.1.2. Quan sát gói tin trên Wireshark

Trong phần này, chúng ta sẽ thử quan sát một gói tin mà Wireshark bắt được. Chúng ta sẽ có các bài thực hành sau để phân tích nội dung cụ thể của các loại gói tin khác nhau.

- Bước 1: Nhập vào bộ lọc xâu **http** chúng ta sẽ thấy trên cửa sổ chỉ hiển thị các gói tin có Protocol là HTTP tương tự như dưới đây. Có thể bỏ qua các gói tin với tên giao thức khác được xây dựng dựa trên HTTP như OCSP

No.	Time	Source	Destination	Protocol	Length	Info
2265	74.019499645	216.58.200.14	192.168.127.138	OCSP	759	Response
3124	85.512587699	192.168.127.138	118.69.16.72	HTTP	350	GET /success.txt HTTP/1.1
3128	85.716399638	118.69.16.72	192.168.127.138	HTTP	438	HTTP/1.1 200 OK (text/plain)
+ 3197	109.331662260	192.168.127.138	104.199.203.54	HTTP	383	GET / HTTP/1.1
+ 3199	109.394251484	104.199.203.54	192.168.127.138	HTTP	6985	HTTP/1.1 200 OK (text/html)
3201	109.568852750	192.168.127.138	104.199.203.54	HTTP	612	GET /static/js/i18n/en/djangojs.b28203373cc1.js HTTP/1.
3203	109.573440569	192.168.127.138	104.199.203.54	HTTP	629	GET /static/css/lms-style-vendor.e94b4f081f3a.css HTTP/1.
3209	109.612285077	104.199.203.54	192.168.127.138	HTTP	1163	HTTP/1.1 200 OK (application/javascript)
3211	109.612485001	192.168.127.138	104.199.203.54	HTTP	624	GET /static/css/lms-main-v1.70875d281f2f.css HTTP/1.1
3213	109.618085897	104.199.203.54	192.168.127.138	HTTP	7441	HTTP/1.1 200 OK (text/css)
3223	109.620468641	192.168.127.138	104.199.203.54	HTTP	611	GET /static/js/lms-main_vendor.b08456a95e51.js HTTP/1.1
3224	109.620613037	192.168.127.138	104.199.203.54	HTTP	611	GET /static/js/lms-application.08b98ee0f748.js HTTP/1.1
3226	109.6207413021	102.168.127.120	104.199.203.54	HTTP	614	GET /static/lms-main_requiered_config_72010aef3bf0.json HTTP/1.1

Frame 3197: 383 bytes on wire (3064 bits), 383 bytes captured (3064 bits) on interface 0  
Ethernet II, Src: VMware\_fd:d5:80 (00:0c:29:fd:d5:80), Dst: VMware\_e2:c5:bd (00:50:56:e2:c5:bd)  
Internet Protocol Version 4, Src: 192.168.127.138, Dst: 104.199.203.54  
Transmission Control Protocol, Src Port: 51036, Dst Port: 80, Seq: 1, Ack: 1, Len: 329  
Hypertext Transfer Protocol

```
0000  00 50 56 e2 c5 bd 00 0c 29 fd d5 80 08 00 45 00  ·PV..... )....E·
0010  01 71 48 78 40 00 40 06 7c de c0 a8 7f 8a 68 c7  ·qHx@. @. |....h·
0020  cb 36 c7 5c 00 50 f8 7c 81 88 78 10 2b 47 50 18  ·6.\-P| ...x +GP·
0030  72 10 75 94 00 00 47 45 54 20 2f 20 48 54 54 50  r.u...GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 63 79 62 65  /1.1.-Ho st: cybe
0050  72 6c 6d 73 66 75 6e 69 78 2e 65 64 75 2e 76  r1ms.fun ix.edu.v
0060  6e 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d  n·User-Agent: M
0070  6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b  ozilla/5.0 (X11;
0080  20 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 20 78  Ubuntu; Linux x
```

- Bước 2: Lựa chọn một gói tin có thông số như sau để quan sát:

Destination: 104.199.203.54

Info: GET / HTTP/1.1

- Bước 3: Chúng ta sẽ thấy cấu trúc gói tin được hiển thị trên vùng 3, còn nội dung gói tin dưới dạng hexa và mã ASCII được hiển thị trên vùng 4. Quan sát ở vùng 3, chúng ta sẽ thấy gói tin này có các tiêu đề đóng gói theo chặng giao thức TCP/IP như sau:

- Tầng liên kết dữ liệu: Ethernet
- Tầng mạng: Internet Protocol version 4 (IPv4)
- Tầng giao vận: Transmission Control Protocol (TCP)
- Tầng ứng dụng: Hypertext Transfer Protocol (HTTP)

## 8.2. Cài đặt Wireshark trên hệ điều hành Windows

Wireshark là một công cụ kiểm tra, theo dõi và phân tích dữ liệu trao đổi giữa máy tính cài đặt công cụ này với các máy tính khác trong mạng. Sau đây, chúng ta sẽ cài đặt Wireshark trên hệ điều hành Windows 10.

Đường dẫn tải về: <https://www.wireshark.org/download.html>

### Download Wireshark

The current stable release of Wireshark is 3.0.3. It supersedes all previous releases. You can also download the latest development release (3.1.0) and documentation.

The screenshot shows the official Wireshark download page. At the top, it says "Stable Release (3.0.3)". Below that, there's a list of download links:

- [Windows Installer \(64-bit\)](#) (highlighted with a red box)
- [Windows Installer \(32-bit\)](#)
- [Windows PortableApps® \(32-bit\)](#)
- [macOS 10.12 and later Intel 64-bit .dmg](#)
- [Source Code](#)

Below these sections are "Old Stable Release (2.6.10)" and "Development Release (3.1.0)", each with a dropdown arrow icon. At the bottom is a "Documentation" section with a dropdown arrow icon.

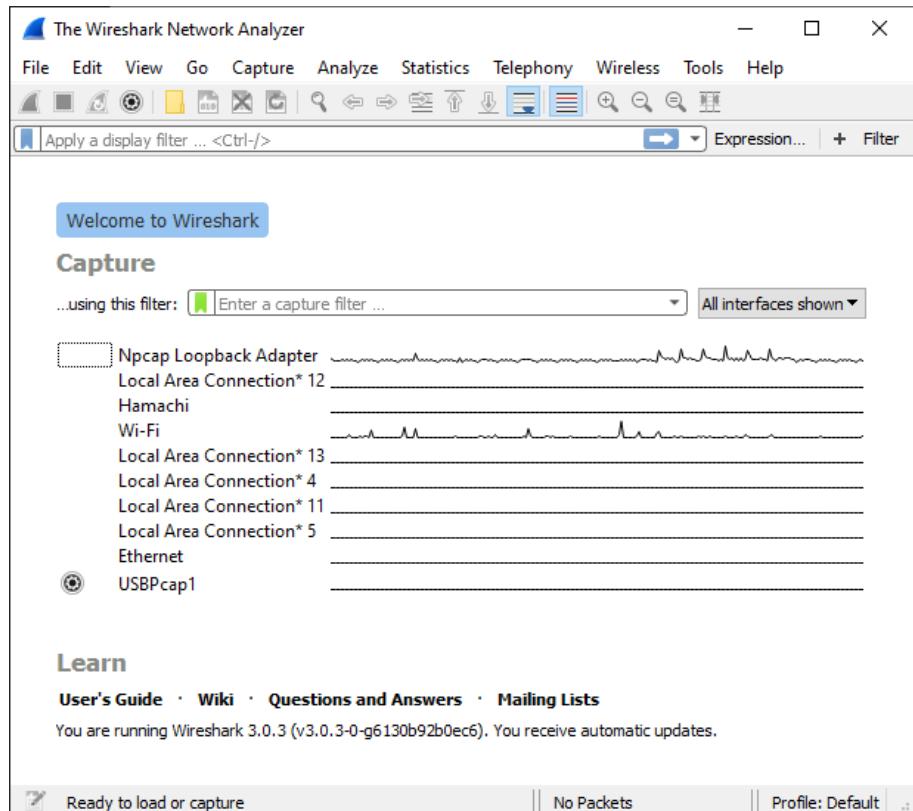
Chúng ta lựa chọn tải về tập tin phù hợp với cấu hình máy tính đang sử dụng, ở đây là **Windows Installer (64-bit)**.

Sau khi tải về thành công, chúng ta mở tập tin **Wireshark-win64-3.0.3.exe** để cài đặt.



### 8.2.1. Giao diện làm việc của Wireshark

- **Bước 1:** Mở Windows Explorer vào đường dẫn cài đặt, khởi động Wireshark (ví dụ đường dẫn mặc định là: C:\Program Files\Wireshark\Wireshark.exe).
- **Bước 2:** Sau khi Wireshark khởi động thành công, các bạn nhìn thấy danh sách các cổng giao tiếp khác nhau trên máy tính mà Wireshark có thể bắt các gói tin trên đó.

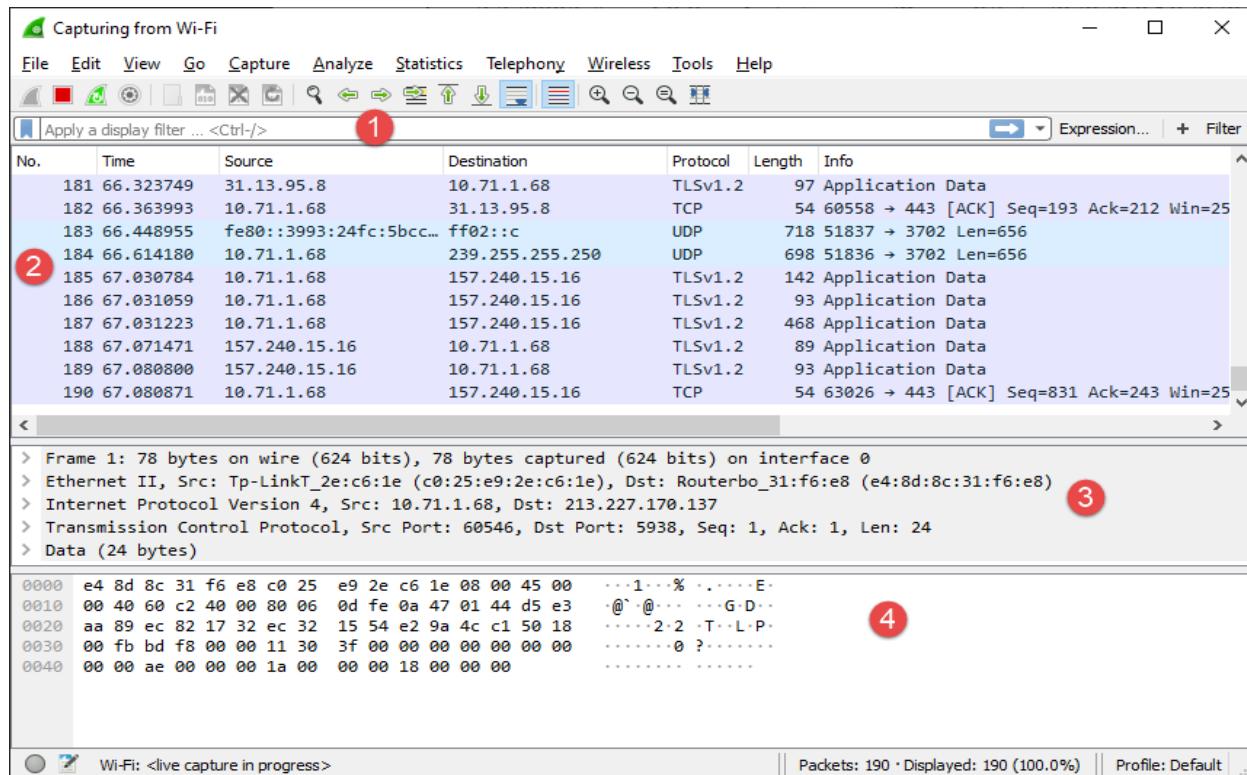


Lưu ý: Để biết các cổng mạng của máy tính, trên cửa sổ Command Prompt gõ lệnh **ipconfig /all**. Như kết quả hiển thị dưới đây, ta có thể thấy cổng mạng của máy tính là Wireless LAN adapter Wi-Fi - TP-Link Wireless USB Adapter

```
C:\WINDOWS\system32\cmd.exe
Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . :
  Description . . . . . : TP-Link Wireless USB Adapter
  Physical Address. . . . . : C0-25-E9-2E-C6-1E
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . : fe80::3993:24fc:5bcc:33da%15(Preferred)
  IPv4 Address. . . . . : 10.71.1.68(Preferred)
  Subnet Mask . . . . . : 255.255.254.0
  Lease Obtained. . . . . : Thursday, August 15, 2019 5:27:27 PM
  Lease Expires . . . . . : Saturday, August 17, 2019 6:10:34 PM
  Default Gateway . . . . . : 10.71.0.1
  DHCP Server . . . . . : 10.71.0.1
  DHCPv6 IAID . . . . . : 79701481
  DHCPv6 Client DUID. . . . . : 00-01-00-01-21-5A-8B-45-48-4D-7E-EA-C2-0A
  DNS Servers . . . . . : 8.8.8.8
                           8.8.4.4
  NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Hamachi:
  Connection-specific DNS Suffix . :
  Description . . . . . : LogMeIn Hamachi Virtual Ethernet Adapter
  Physical Address. . . . . : 02-50-F2-65-32-00
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Default Gateway . . . . . : 25.0.0.1
```

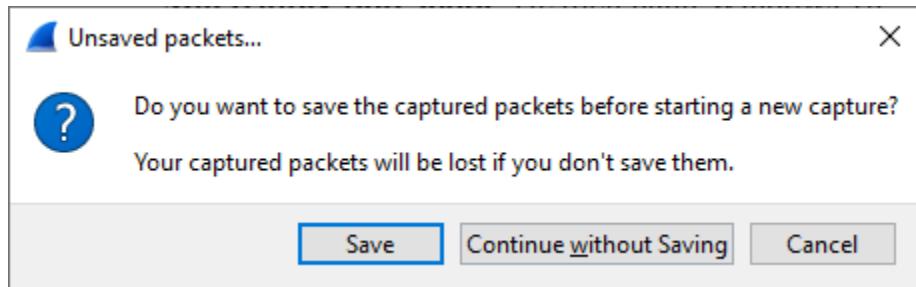
- **Bước 3:** Nhấp đúp vào cổng mạng, chúng ta sẽ thấy giao diện làm việc của Wireshark như sau:



- Thanh công cụ: Xem mục **Help** của phần mềm để biết thêm chi tiết
- Vùng 1: Tạo bộ lọc cho phép quan sát các gói tin thỏa mãn yêu cầu nào đó
- Vùng 2: Danh sách các gói tin đã bắt.
  - ❖ **No.:** Số thứ tự gói tin
  - ❖ **Time:** thời điểm bắt (tính bằng giây kể từ khi bắt đầu)
  - ❖ **Source:** Địa chỉ nguồn của gói tin
  - ❖ **Destination:** Địa chỉ đích của gói tin
  - ❖ **Protocol:** Giao thức.
  - ❖ **Length:** Kích thước
  - ❖ **Info:** các thông tin chính về gói tin (thường lấy từ header của gói tin)
- Vùng 3: Các nội dung phân tích được ở tất cả các tầng trong mô hình TCP/IP.
- Vùng 4: Nội dung thực tế của gói tin

- **Bước 4:** Mở trình duyệt và truy cập vào trang <http://cyberlms.funix.edu.vn>

- **Bước 5:** Ngừng bắt gói tin bằng cách nhấp vào biểu tượng trên thanh công cụ. Chúng ta có thể lưu dữ liệu bắt được vào tệp tin có định dạng **.pcapng**.



### 8.2.2. Quan sát gói tin trên Wireshark

Trong phần này, chúng ta sẽ thử quan sát một gói tin mà Wireshark bắt được. Chúng ta sẽ có các bài thực hành sau để phân tích nội dung cụ thể của các loại gói tin khác nhau.

- Bước 1: Nhập vào bộ lọc xâu **http** chúng ta sẽ thấy trên cửa sổ chỉ hiển thị các gói tin có Protocol là HTTP tương tự như dưới đây. Có thể bỏ qua các gói tin với tên giao thức khác được xây dựng dựa trên HTTP như OCSP.

No.	Time	Source	Destination	Protocol	Length	Info
115	60.888446	5.45.58.216	10.71.1.68	HTTP	101	HTTP/1.1 200 OK
116	60.884065	10.71.1.68	5.45.58.216	HTTP	344	GET /R/A28KIGQ4YjQxY2U50DAzYTQyZjFiOTQ5YWY5ZjQ1ZD
162	66.837050	10.71.1.68	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
164	66.870080	13.107.4.52	10.71.1.68	HTTP	566	HTTP/1.1 200 OK (text/plain)
1087	248.455004	10.71.1.68	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
1091	248.511971	13.107.4.52	10.71.1.68	HTTP	566	HTTP/1.1 200 OK (text/plain)

```

> Frame 115: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface 0
> Ethernet II, Src: Routerbo_31:f6:e8 (e4:8d:8c:31:f6:e8), Dst: Tp-LinkT_2e:c6:1e (c0:25:e9:2e:c6:1e)
> Internet Protocol Version 4, Src: 5.45.58.216, Dst: 10.71.1.68
> Transmission Control Protocol, Src Port: 80, Dst Port: 49885, Seq: 1615, Ack: 1, Len: 47
> [3 Reassembled TCP Segments (1661 bytes): #112(154), #113(1460), #115(47)]
> Hypertext Transfer Protocol
> Data (1489 bytes)

0000  03 20 08 d1 03 12 01 ff 32 18 08 04 10 c1 97 e0  . .... 2.....
0010  72 18 80 0a 20 c9 f6 fa f3 c9 2d 28 c9 f6 fa f3  r.....(....
0020  c9 2d 0a ac 0b 41 53 55 21 56 50 53 7a 00 17 08  ....ASU !VPSz...
0030  19 63 00 00 00 4c 05 00 00 7c 05 00 00 78 da 35  .c...L...|...x..5
0040  92 7b 38 d4 69 14 c7 cf cc 34 72 6b d3 30 b9 ac  .{8.i...4rk.0..
0050  fb a5 1d 8d 32 29 97 62 23 83 c8 b8 4e 45 91 d8  ....2).b #.NE..
0060  58 69 30 45 ee 26 3f 52 ae 53 aa 91 72 57 a1 5a  XioE.&?R .S..rW.Z

Frame (101bytes) Reassembled TCP (1661bytes) De-chunked entity body (1489 bytes)
wireshark_Wi-Fi_20190817143241_a02384.pcapng || Packets: 1539 · Displayed: 8 (0.5%) || Profile: Default ...

```

- Bước 2: Lựa chọn một gói tin có thông số như sau để quan sát:

Destination: 10.71.1.68

Info: HTTP/1.1 200 OK

- Bước 3: Chúng ta sẽ thấy cấu trúc gói tin được hiển thị trên vùng 3, còn nội dung gói tin dưới dạng HEXA và mã ASCII được hiển thị trên vùng 4. Quan sát ở vùng 3, chúng ta sẽ thấy gói tin này có các tiêu đề đóng gói theo chia giao thức TCP/IP như sau:

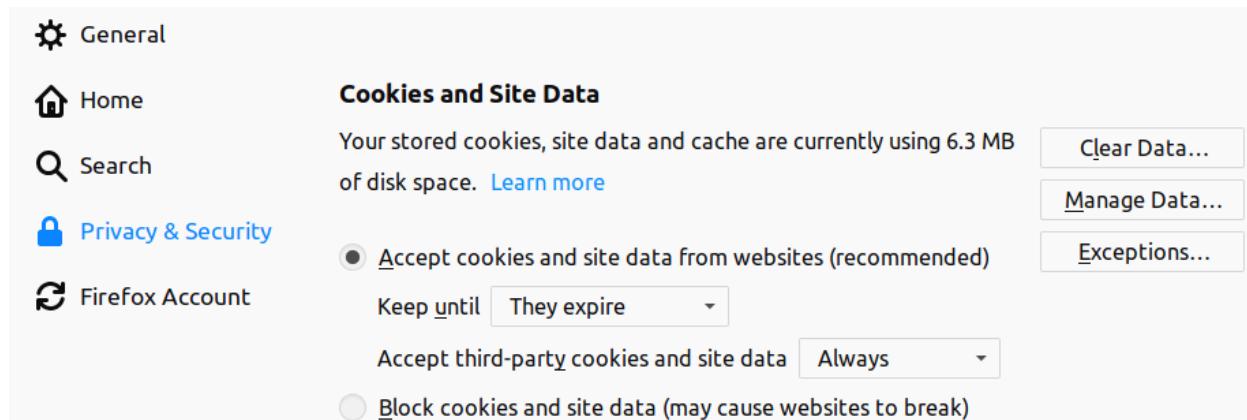
- Tầng liên kết dữ liệu: Ethernet
- Tầng mạng: Internet Protocol version 4 (IPv4)
- Tầng giao vận: Transmission Control Protocol (TCP)
- Tầng ứng dụng: Hypertext Transfer Protocol (HTTP)

## 5. PHỤ LỤC 2: PHÂN TÍCH KHUNG TIN ETHERNET

### 9.1. Phân tích khung tin Ethernet trên Ubuntu

#### 9.1.1. Sử dụng Wireshark để bắt gói tin

- **Bước 1:** Mở trình duyệt Firefox và xóa bộ đệm của ứng dụng như sau
- Nhấn chuột vào biểu tượng  ở góc trên bên phải
  - Chọn Preferences
  - Trong mục Privacy & Security, nhấn nút Clear Data



- Chọn mục Cached Web Content và nhấn nút Clear
- **Bước 2:** Khởi động công cụ Wireshark từ cửa sổ Terminal với lệnh **sudo wireshark**
- **Bước 3:** Bắt đầu bắt gói tin trên các mạng với Wireshark
- **Bước 4:** Mở cửa sổ Terminal thứ 2 và gõ lệnh sau:

```
student@ubuntu:~/Documents$ sudo ip -s -s neigh flush all
```

- **Bước 5:** Trên trình duyệt Firefox, truy cập vào trang <http://nct.soict.hust.edu.vn>. Sau khi trang Web được tải về. Dùng bắt gói tin trên Wireshark. Kết quả bắt gói tin trên Wireshark tương tự như sau:

Figure 1: Network traffic capture from 'ethernet.pcapng' showing a series of SYN and ACK requests between host 192.168.127.138 and host 192.168.127.2.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.127.2? Tell 192.168.127.1
2	0.876848487	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.127.2? Tell 192.168.127.1
3	1.877541968	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.127.2? Tell 192.168.127.1
4	2.416508031	Vmware_fd:d5:80	Broadcast	ARP	42	Who has 192.168.127.2? Tell 192.168.127.138
5	2.417021218	Vmware_e2:c5:bd	Vmware_fd:d5:80	ARP	60	192.168.127.2 is at 00:50:56:e2:c5:bd
6	2.417029130	192.168.127.138	104.199.203.54	TCP	74	42360 -> [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK P=0
7	2.484723025	104.199.203.54	192.168.127.138	TCP	60	80 -> 42360 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK P=0
8	2.484789091	192.168.127.138	104.199.203.54	TCP	54	42360 -> 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
9	2.485102146	192.168.127.138	104.199.203.54	HTTP	620	GET / HTTP/1.1
10	2.486277305	104.199.203.54	192.168.127.138	TCP	60	80 -> 42360 [ACK] Seq=1 Ack=567 Win=64240 Len=0
11	2.661301210	104.199.203.54	192.168.127.138	HTTP	6985	HTTP/1.1 200 OK (text/html)
12	2.661351855	192.168.127.138	104.199.203.54	TCP	54	42360 -> [ACK] Seq=567 Ack=6932 Win=42340 Len=0
13	2.899820651	192.168.127.138	104.199.203.54	HTTP	612	GET /static/js/i18n/en/djangojs.b28203373cc1.js HTTP/1.1
14	2.900188822	104.199.203.54	192.168.127.138	TCP	60	80 -> 42360 [ACK] Seq=6932 Ack=1125 Win=64240 Len=0
15	2.900715596	192.168.127.138	104.199.203.54	TCP	74	42362 -> 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK P=0
16	2.905487873	192.168.127.138	104.199.203.54	TCP	74	42364 -> 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK P=0
17	2.909637027	192.168.127.138	104.199.203.54	TCP	74	42366 -> 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK P=0

### **Lưu ý:**

- Nếu trên máy học viên không bắt được các gói tin có Protocol là ARP thì nên thực hiện lại từ bước 1.
  - Các gói tin bắt được trên máy các bạn có thể sẽ có thông số khác. Điều này là hoàn toàn bình thường và không có ảnh hưởng tới quá trình thực hành

### 9.1.2. Phân tích lưu lượng

*Lưu ý: Các giá trị phân tích dưới đây chỉ mang tính chất minh họa. Với lưu lượng bắt trên máy sinh viên, kết quả có thể sẽ khác. Các bạn có thể download file lưu lượng mẫu tại địa chỉ sau cho nội dung minh họa dưới đây:*

<https://drive.google.com/file/d/1Lk2PJ6m-7nmc4hIfeDoaf-V7akShVchz>

- **Bước 1:** Chọn một gói tin có Protocol mà ARP và Destination là Broadcast
  - **Bước 2:** Mở rộng phần tiêu đề Ethernet II như sau.

Chúng ta sẽ thấy trường Destination có giá trị là ff:ff:ff:ff:ff:ff. Đây chính là địa chỉ MAC quảng bá. Như vậy, gói tin này đã được gửi đi theo phương thức quảng bá.

- **Bước 3:** Trên cửa sổ Terminal, thực hiện lệnh **ip a**, chúng ta nhận được danh sách các cạc mạng đang có trên máy tính. Kết quả tương tự như sau:

```
student@ubuntu:~/Documents$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:fd:d5:80 brd ff:ff:ff:ff:ff:ff
    inet 192.168.127.138/24 brd 192.168.127.255 scope global dynamic noprefixroute ens33
        valid_lft 1368sec preferred_lft 1368sec
    inet6 fe80::9608:58e8:2eba:a6a6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Trong kết quả minh họa trên, ta thấy cạc mạng số 2 là ens33 có địa chỉ MAC là 00:0c:29:fd:d5:80. Đối chiếu với trường Source trong tiêu đề Ethernet của gói tin trên, ta có thể thấy đây chính là giá trị của trường đó. Như vậy gói tin quảng bá mà chúng ta vừa phân tích được gửi đi trên chính máy tính này.

- **Bước 4:** Trên Wireshark chọn gói tin có các thông số như sau:

- Destination: 104.199.203.54
- Protocol: HTTP
- Info: GET / HTTP/1.1

Đây chính là gói tin được gửi đi từ máy của bạn tới máy chủ có tên miền nct.soict.hust.edu.vn

- **Bước 5:** Trên cửa sổ Wireshark mở rộng phần tiêu đề Ethernet II.

S	E	Source	Destination	Type	Length	Protocol
9	2.485102146	192.168.127.138	104.199.203.54	HTTP	620	GET / HTTP/1.1
10	2.486277305	104.199.203.54	192.168.127.138	TCP	60	80 → 42360 [ACK]
11	2.661301210	104.199.203.54	192.168.127.138	HTTP	6985	HTTP/1.1 200 OK
12	2.661351855	192.168.127.138	104.199.203.54	TCP	54	42360 → 80 [ACK]
13	2.899820651	192.168.127.138	104.199.203.54	HTTP	612	GET /static/js/i
14	2.900188822	104.199.203.54	192.168.127.138	TCP	60	80 → 42360 [ACK]
15	2.900715596	192.168.127.138	104.199.203.54	TCP	74	42362 → 80 [SYN]
16	2.905487873	192.168.127.138	104.199.203.54	TCP	74	42364 → 80 [SYN]
17	2.909637027	192.168.127.138	104.199.203.54	TCP	74	42366 → 80 [SYN]

Frame 9: 620 bytes on wire (4960 bits), 620 bytes captured (4960 bits) on interface 0  
**Ethernet II, Src: Vmware\_fd:d5:80 (00:0c:29:fd:d5:80), Dst: Vmware\_e2:c5:bd (00:50:56:e2:c5:  
 ► Destination: Vmware\_e2:c5:bd (00:50:56:e2:c5:bd)  
 ► Source: Vmware\_fd:d5:80 (00:0c:29:fd:d5:80)  
 Type: IPv4 (0x0800)**  
 Internet Protocol Version 4 Src: 192.168.127.138 Dst: 104.199.203.54

Rất dễ để nhận thấy, địa chỉ MAC nguồn của gói tin này là địa chỉ máy tính của bạn. Tuy nhiên, địa chỉ MAC đích không phải là địa chỉ của máy chủ nct.soict.hust.edu.vn. Chúng ta sẽ đề cập đến điều này trong những bài học sau.

Trường Type ghi nhận giá trị 0x0800 chính là số hiệu của giao thức IP theo chuẩn Ethernet. Như vậy có thể thấy, khung tin Ethernet này mang theo trong phần Payload của nó một gói tin IPv4.

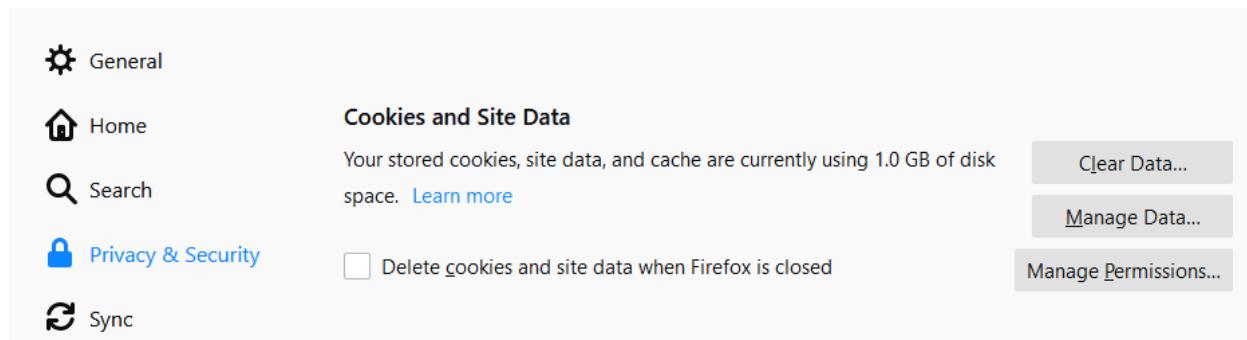
Chúng ta có thể để ý thêm phần nội dung của gói tin có xâu “GET / HTTP/1.1” và “nct.soict.hust.edu.vn”. Đây chính là dữ liệu của dịch vụ Web. Trong các bài học sau, chúng sẽ phân tích rõ hơn.

- **Bước 6:** Chọn gói tin mà máy chủ nct.soict.hust.edu.vn gửi lại cho máy tính của chúng ta và thực hiện các bước phân tích tương tự trên. Các bạn có thể tự luyện tập để xác định các thông số trên tiêu đề Ethernet II của gói tin.

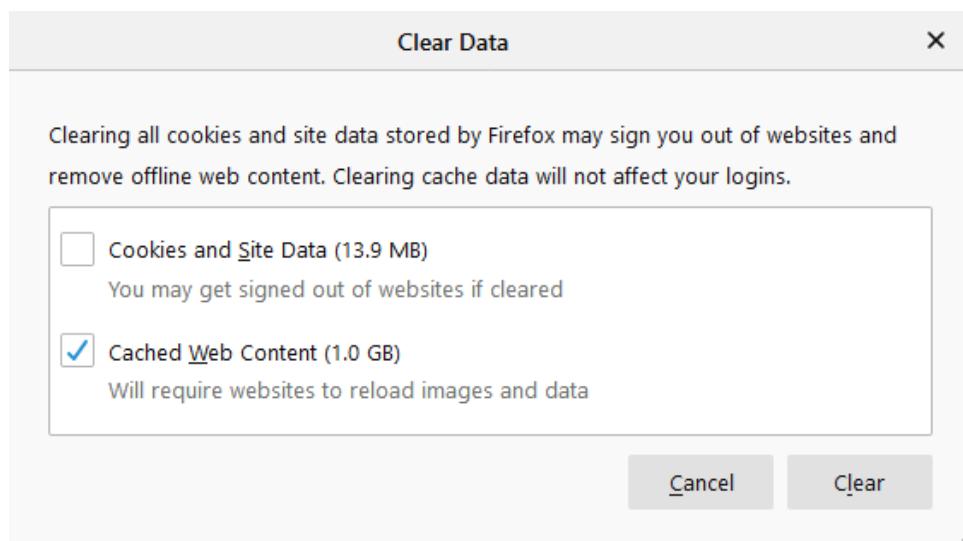
## 9.2. Phân tích khung tin Ethernet trên Windows

### 9.2.1. Sử dụng Wireshark để bắt gói tin

- **Bước 1:** Mở trình duyệt Firefox và xóa bộ đệm của ứng dụng như sau:
  - Nhấn chuột vào biểu tượng  ở góc trên bên phải.
  - Chọn *Options*.
  - Trong mục *Privacy & Security*, tìm mục *Cookies and Site Data* nhấn nút *Clear Data*.



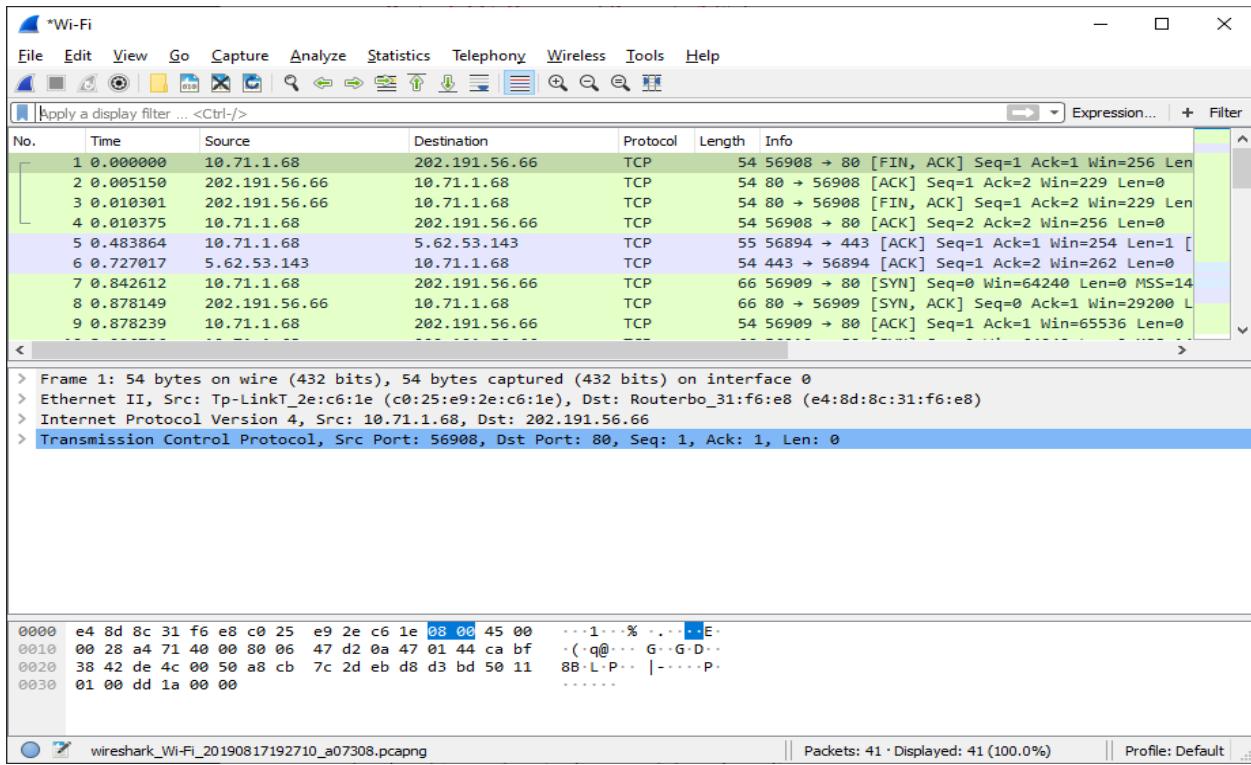
- Chọn mục *Cached Web Content* và nhấn nút *Clear*.



- **Bước 2:** Mở Windows Explorer vào đường dẫn cài đặt, khởi động Wireshark (ví dụ đường dẫn mặc định là: C:\Program Files\Wireshark\Wireshark.exe).
- **Bước 3:** Bắt đầu bắt gói tin trên cổng mạng với Wireshark.
- **Bước 4:** Mở Command Prompt với quyền quản trị Administrator (Nhấn Windows + X, chọn Command Prompt (Admin) gõ lệnh sau:

```
C:\WINDOWS\system32>netsh interface ip delete arpcach
ok.
```

- **Bước 5:** Trên trình duyệt Firefox, truy cập vào trang http://nct.soict.hust.edu.vn. Sau khi trang Web được tải về. Dừng bắt gói tin trên Wirshark. Kết quả bắt gói tin trên Wireshark tương tự như sau:



### Lưu ý:

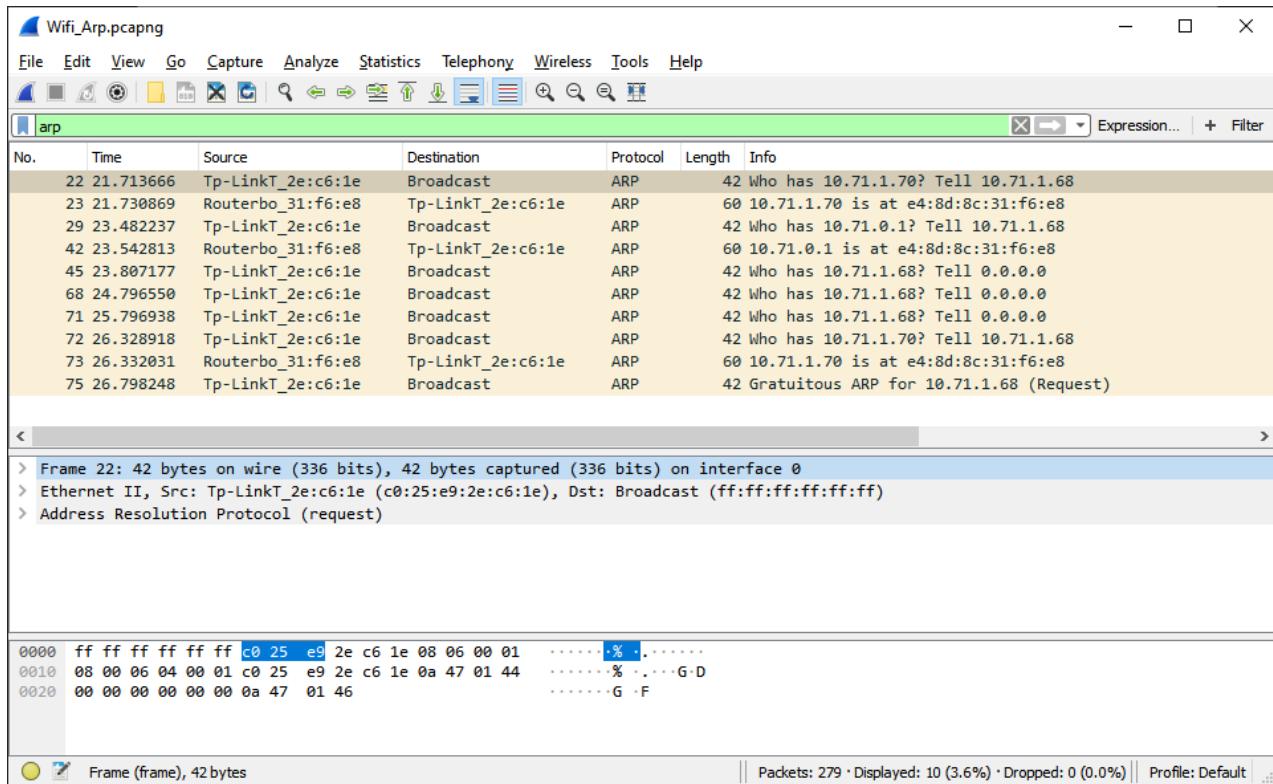
- Nếu trên máy học viên không bắt được các gói tin có Protocol là ARP thì nên thực hiện lại từ bước 1.
- Các gói tin bắt được trên máy các bạn có thể sẽ có thông số khác. Điều này là hoàn toàn bình thường và không có ảnh hưởng tới quá trình thực hành.

### 9.2.2. Phân tích lưu lượng

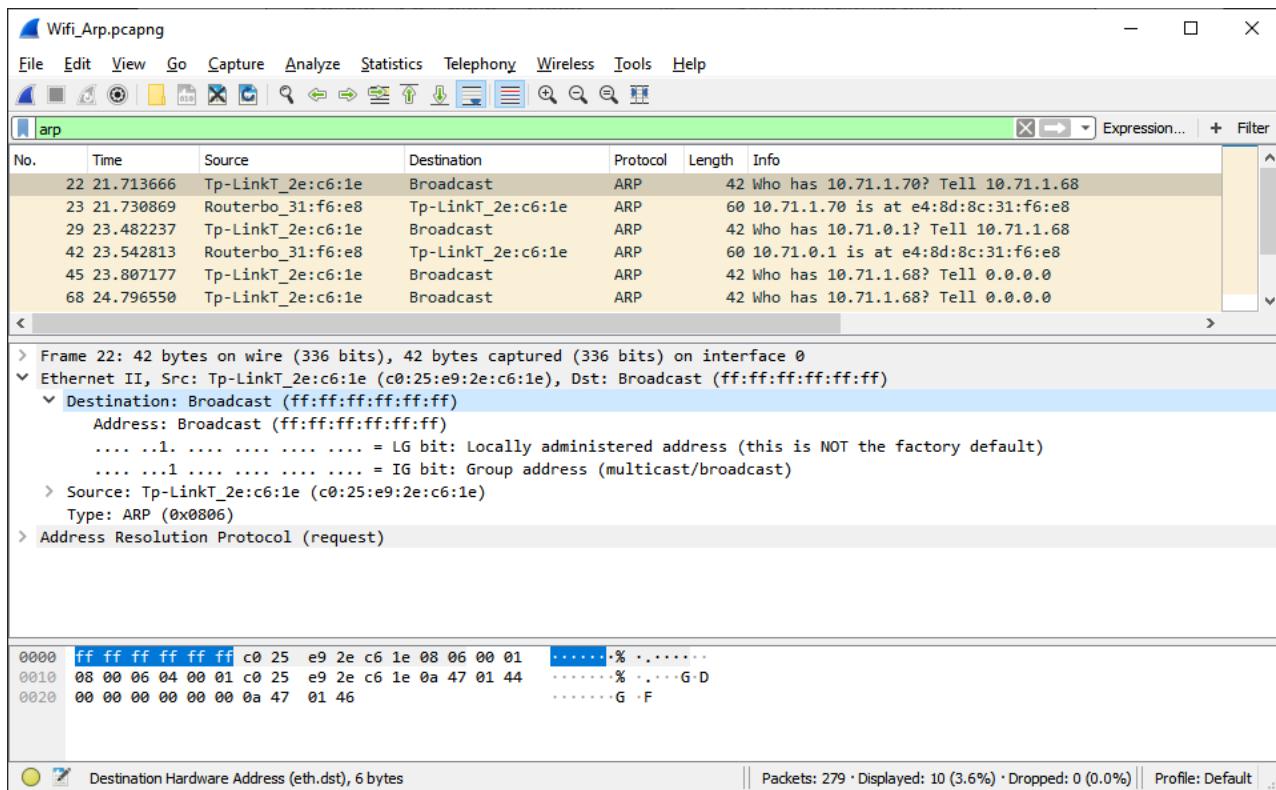
**Lưu ý:** Các giá trị phân tích dưới đây chỉ mang tính chất minh họa. Với lưu lượng bắt trên máy sinh viên, kết quả có thể sẽ khác. Các bạn có thể download file lưu lượng mẫu tại địa chỉ sau cho nội dung minh họa dưới đây:

<https://drive.google.com/file/d/1Lk2PJ6m-7nmc4hJfeDoaf-V7akShVchz>

- **Bước 1:** Chọn một gói tin có **Protocol** là **ARP** và **Destination** là **Broadcast** (Filter từ khóa arp).



- **Bước 2:** Mở rộng phần tiêu đề Ethernet II như sau:



Chúng ta sẽ thấy trường Destination có giá trị là ff:ff:ff:ff:ff:ff. Đây chính là địa chỉ MAC quảng bá. Như vậy, gói tin này đã được gửi đi theo phương thức quảng bá.

- **Bước 3:** Trên cửa sổ Command Prompt, thực hiện lệnh **ipconfig /all**, chúng ta nhận được danh sách các cạc mạng đang có trên máy tính. Kết quả tương tự như sau:

```
C:\WINDOWS\system32\cmd.exe
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
Description . . . . . : TP-Link Wireless USB Adapter
Physical Address. . . . . : C0-25-E9-2E-C6-1E
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::3993:24fc:5bcc:33da%15(PREFERRED)
IPv4 Address. . . . . : 10.71.1.68(PREFERRED)
Subnet Mask . . . . . : 255.255.254.0
Lease Obtained. . . . . : Thursday, August 15, 2019 5:27:27 PM
Lease Expires . . . . . : Saturday, August 17, 2019 6:10:34 PM
Default Gateway . . . . . : 10.71.0.1
DHCP Server . . . . . : 10.71.0.1
DHCPv6 IAID . . . . . : 79701481
DHCPv6 Client DUID. . . . . : 00-01-00-01-21-5A-8B-45-48-4D-7E-EA-C2-0A
DNS Servers . . . . . : 8.8.8.8
                                         8.8.4.4
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Hamachi:

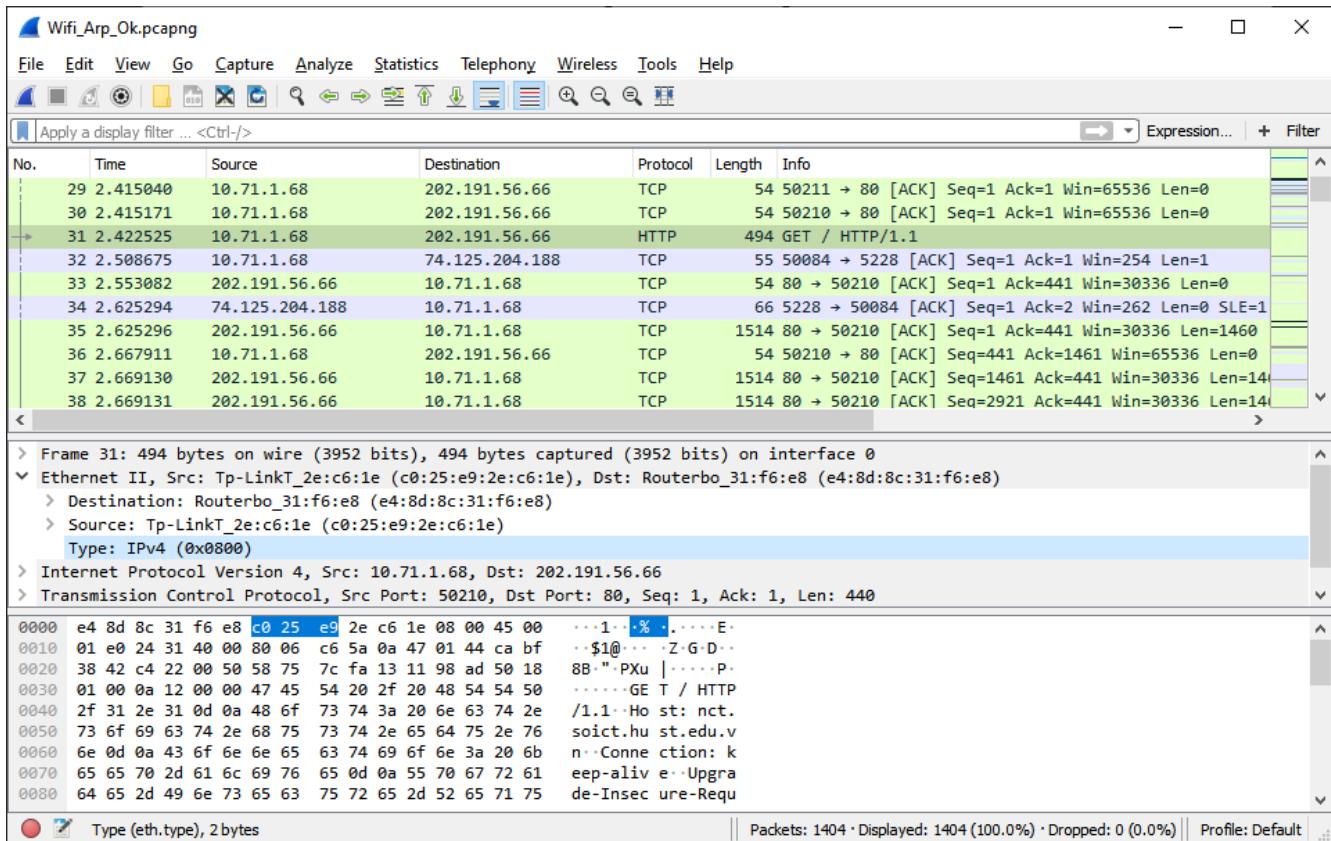
Connection-specific DNS Suffix . :
Description . . . . . : LogMeIn Hamachi Virtual Ethernet Adapter
Physical Address. . . . . : 02-50-F2-65-32-00
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Default Gateway . . . . . : 25.0.0.1
```

Trong kết quả minh họa trên, ta thấy các mạng Wireless LAN adapter Wi-Fi là TP-Link Wireless Wireless USB Adapter có địa chỉ MAC là C0-25-E9-2E-C6-1E. Đối chiếu với trường Source trong tiêu đề Ethernet của gói tin trên, ta có thể thấy đây chính là giá trị của trường đó. Như vậy gói tin quảng bá mà chúng ta vừa phân tích được gửi đi trên chính máy tính này.

- **Bước 4:** Trên Wireshark chọn gói tin có các thông số như sau:
  - Destination: 202.191.56.66
  - Protocol: HTTP
  - Info: GET / HTTP/1.1

Đây chính là gói tin được gửi đi từ máy của bạn tới máy chủ có tên miền nct.soict.hust.edu.vn.

- **Bước 5:** Trên cửa sổ Wireshark mở rộng phần tiêu đề Ethernet II.



Rất dễ để nhận thấy, địa chỉ MAC nguồn của gói tin này là địa chỉ máy tính của bạn. Tuy nhiên, địa chỉ MAC đích không phải là địa chỉ của máy chủ nct.soiict.hust.edu.vn. Chúng ta sẽ đề cập đến điều này trong những bài học sau.

Trường Type ghi nhận giá trị 0x0800 chính là số hiệu của giao thức IP theo chuẩn Ethernet. Như vậy có thể thấy, khung tin Ethernet này mang theo trong phần Payload của nó một gói tin IPv4.

Chúng ta có thể để ý thêm phần nội dung của gói tin có xâu “GET / HTTP/1.1” và “nct.soiict.hust.edu.vn”. Đây chính là dữ liệu của dịch vụ Web. Trong các bài học sau, chúng sẽ phân tích rõ hơn.

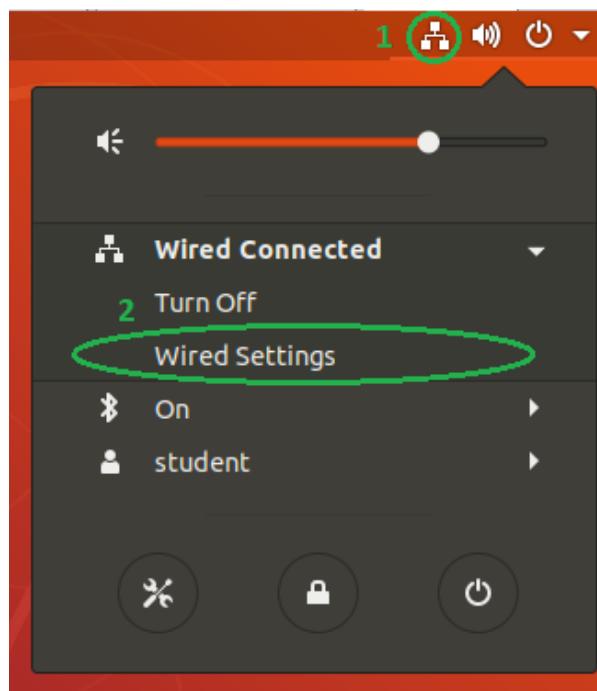
- **Bước 6:** Chọn gói tin mà máy chủ nct.soiict.hust.edu.vn gửi lại cho máy tính của chúng ta và thực hiện các bước phân tích tương tự trên. Các bạn có thể tự luyện tập để xác định các thông số trên tiêu đề Ethernet II của gói tin.

## 6. PHỤ LỤC 3: PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC IP VÀ ARP

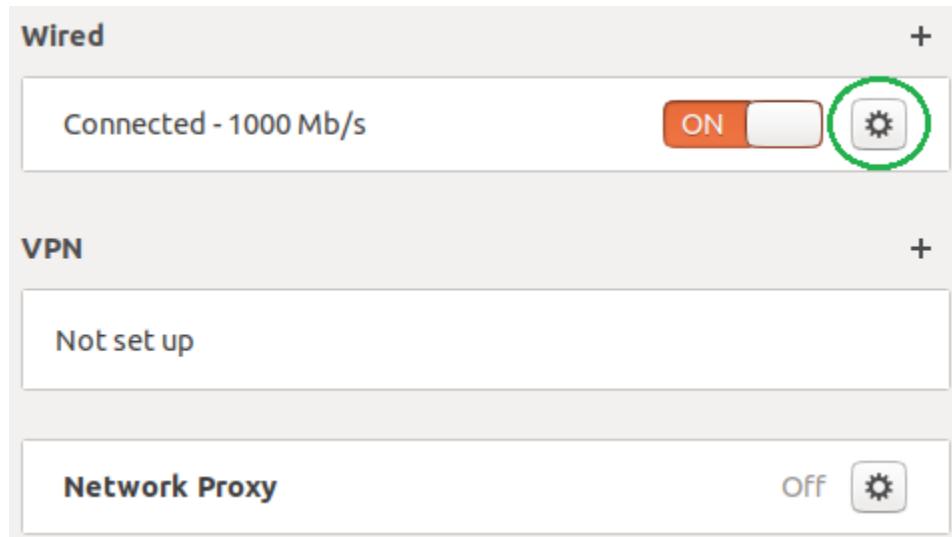
### 10.1. Phân tích hoạt động trên môi trường Ubuntu

#### 10.1.1. Cấu hình các thông số địa chỉ IP cho máy trạm

- **Bước 1:** Để không làm gián đoạn kết nối mạng của máy trạm, trước tiên ta tìm xem máy trạm đang sử dụng địa chỉ IP nào. Chọn biểu tượng kết nối mạng ở góc trên bên phải của màn hình. Chọn tiếp mục Wired Settings



- **Bước 2:** Nhấn vào biểu tượng Setting trong mục Wired



- **Bước 3:** Chúng ta có thể thấy các thông số địa chỉ IP mà máy tính đang sử dụng. Ví dụ minh họa như hình dưới đây.



Các thông số này bao gồm:

- IP Address(Địa chỉ IP): 192.168.127.138. Địa chỉ này không kèm mặt nạ mạng nên có thể coi đó là địa chỉ phân lớp. Để thấy đây là địa chỉ phân lớp C nên có số bit mặc định của Network ID là 24.
- Default Router (Router mặc định): 192.168.127.2
- DNS (Địa chỉ máy chủ DNS): 192.168.127.2

- **Bước 4:** Chọn mục IPv4 của cửa sổ trên và điền các thông số mà chúng ta đã thấy ở bước trên như sau. Nhấn nút Apply sau khi đã thiết lập xong

Address	Netmask	Gateway
192.168.127.138	24	192.168.127.2

**DNS**

Automatic

8.8.8.8, 1.1.1.1

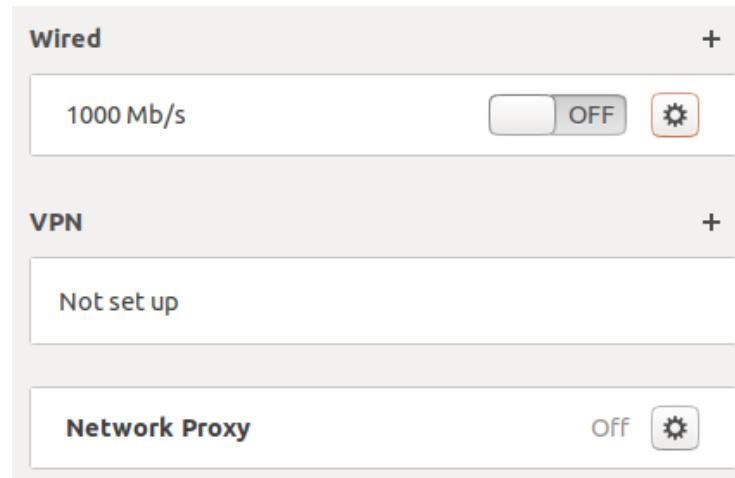
Separate IP addresses with commas

**Routes**

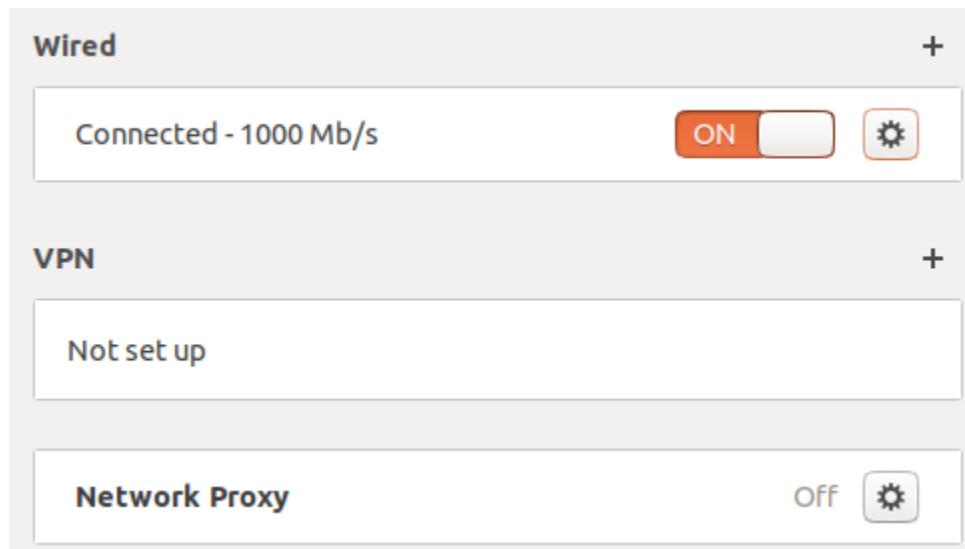
Automatic

Address	Netmask	Gateway	Metric

- **Bước 5:** Gạt nút ON/OFF sang vị trí OFF.



Sau đó gạt lại sang vị trí ON để khởi động lại cạc mạng.



- **Bước 6:** Trên cửa sổ Terminal, chúng ta có thể sử dụng lệnh **ip a** để xem thông tin cấu hình địa chỉ IP của máy trạm:

```
student@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:fd:d5:80 brd ff:ff:ff:ff:ff:ff
    inet 192.168.127.138/24 brd 192.168.127.255 scope global dynamic noprefixroute ens33
        valid_lft 955sec preferred_lft 955sec
    inet6 fe80::9608:58e8:2eba:a6a6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

- **Bước 6:** Chúng ta có thể truy cập vào website bất kỳ để kiểm chứng các thiết lập trên là chính xác hay không.

### 10.1.2. Sử dụng Wireshark để bắt gói tin

- **Bước 1:** Khởi động công cụ Wireshark từ cửa sổ Terminal với lệnh **sudo wireshark**
- **Bước 3:** Bắt đầu bắt gói tin trên các mạng phù hợp với Wireshark
- **Bước 4:** Mở cửa sổ Terminal thứ 2 và gõ lệnh sau để xóa bảng ARP Table của máy trạm:

```
student@ubuntu:~/Documents$ sudo ip -s -s neigh flush all
```

- **Bước 5:** Trên cửa sổ Terminal thực hiện lệnh ping 1.1.1.1 -s 2000 -c 4 như sau:

```
student@ubuntu:~/Documents$ ping 1.1.1.1 -s 2000 -c 4
```

Khi lệnh này thực hiện xong, dừng bắt gói tin. Trên cửa sổ của Wireshark, chúng ta sẽ thấy các gói tin tương tự như sau:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.127.2? Tell 192.168.127.1
2	0.711937838	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.127.2? Tell 192.168.127.1
3	1.747860909	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.127.2? Tell 192.168.127.1
4	2.269398050	192.168.127.1	192.168.127.255	DB-LSP...	199	Dropbox LAN sync Discovery Protocol
5	3.002508560	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.127.2? Tell 192.168.127.1
6	3.440399522	192.168.127.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
7	3.712293981	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.127.2? Tell 192.168.127.1
8	4.243860886	Vmware_fd:d5:80	Broadcast	ARP	42	Who has 192.168.127.2? Tell 192.168.127.138
9	4.244362212	Vmware_e2:c5:bd	Vmware_fd:d5:80	ARP	60	192.168.127.2 is at 00:50:56:e2:c5:bd
10	4.244371101	192.168.127.138	1.1.1.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0,
11	4.244398655	192.168.127.138	1.1.1.1	ICMP	562	Echo (ping) request id=0x0efd, seq=1/256, 1
12	4.308459590	1.1.1.1	192.168.127.138	IPv4	562	Fragmented IP protocol (proto=ICMP 1, off=14
13	4.308490886	1.1.1.1	192.168.127.138	ICMP	1514	Echo (ping) reply id=0x0efd, seq=1/256, 1

- **Bước 6:** Sử dụng lệnh **ip n** để xem thông tin bảng ARP Table

```
student@ubuntu:~$ ip n
192.168.127.2 dev ens33 lladdr 00:50:56:e2:c5:bd STALE
```

### **Lưu ý:**

- Nếu trên máy học viên không bắt được các gói tin có Protocol là ARP thì nên thực hiện lại từ bước 1.
  - Các gói tin bắt được trên máy các bạn có thể sẽ có thông số khác. Điều này là hoàn toàn bình thường và không có ảnh hưởng tới quá trình thực hành

### **10.1.3. Phân tích lưu lượng**

*Lưu ý: Các giá trị phân tích dưới đây chỉ mang tính chất minh họa. Với lưu lượng bắt trên máy sinh viên, kết quả có thể sẽ khác. Các bạn có thể download file lưu lượng mẫu tại địa chỉ sau cho nội dung minh họa dưới đây:*

<https://drive.google.com/file/d/1iFg6Y3sk5fS1tC3FdGHPVPlQhfI3y4Z>

- **Bước 1:** Bạn có thể thấy trên file lưu lượng bắt được một số gói tin có Protocol là ARP và địa chỉ nguồn là địa chỉ máy của bạn. Mở rộng phần tiêu đề Address Resolution Protocol, chúng ta có thể thấy đây là gói tin ARP Request.

7	3.712293981	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.127.2? Tell 192.168.127.1
8	4.243860886	Vmware_fd:d5:80	Broadcast	ARP	42	Who has 192.168.127.2? Tell 192.168.127.188
9	4.244362212	Vmware_e2:c5:bd	Vmware_fd:d5:80	ARP	60	192.168.127.2 is at 00:50:56:e2:c5:bd
10	4.244371101	192.168.127.138	1.1.1.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0)
11	4.244398655	192.168.127.138	1.1.1.1	ICMP	562	Echo (ping) request id=0x0efd, seq=1/256, t
12	4.308459590	1.1.1.1	192.168.127.138	IPv4	562	Fragmented IP protocol (proto=ICMP 1, off=1)
13	4.308490886	1.1.1.1	192.168.127.138	ICMP	1514	Echo (ping) reply id=0x0efd, seq=1/256, t
14	4.46560616	192.168.127.1	255.255.255.255	ICMP	616	NOP ICMP

▼ Ethernet II, Src: Vmware\_fd:d5:80 (00:0c:29:fd:d5:80), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- ▶ Source: Vmware\_fd:d5:80 (00:0c:29:fd:d5:80)
- Type: ARP (0x0806)

▼ Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: Vmware\_fd:d5:80 (00:0c:29:fd:d5:80)
- Sender IP address: 192.168.127.138
- Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Target IP address: 192.168.127.2

Các thông tin chúng ta đọc được từ phần tiêu đề này gồm có:

- Hardware type: Chuẩn phần cứng sử dụng trong ví dụ này là Ethernet
  - Protocol type: giao thức là IPv4
  - Hardware size: kích thước phần cứng là 6 byte (địa chỉ MAC)
  - Protocol size: địa chỉ giao thức tầng trên là 4 byte
  - Sender MAC address: địa chỉ MAC nút nguồn
  - Sender IP address: địa chỉ IP của nút nguồn
  - Target MAC address: địa chỉ MAC cần tìm kiếm
  - Target IP address: địa chỉ IP đã biết

- Bước 2:** Tiếp theo, bạn sẽ thấy gói tin trả lời là gói tin ARP có địa chỉ đích là địa chỉ MAC máy tính của bạn. Các thông tin trong gói này tương tự ở trên, với điểm khác biệt là địa chỉ Target MAC address đã là địa chỉ cần tìm kiếm. Các bạn có thể thấy rằng, đây cũng chỉ là địa chỉ nguồn của khung tin Ethernet mang theo gói ARP Reply trả lời.

8	4.243860886	Vmware_fd:d5:80	Broadcast	ARP	42 Who has 192.168.127.
9	4.244362212	Vmware_e2:c5:bd	Vmware_fd:d5:80	ARP	60 192.168.127.2 is at
10	4.244371101	192.168.127.138	1.1.1.1	IPv4	1514 Fragmented IP protocol
11	4.244398655	192.168.127.138	1.1.1.1	ICMP	562 Echo (ping) request
12	4.308459590	1.1.1.1	192.168.127.138	IPv4	562 Fragmented IP protocol
13	4.308490886	1.1.1.1	192.168.127.138	ICMP	1514 Echo (ping) reply
14	4.442563816	192.168.127.1	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1
15	4.711802620	Vmware_c0:00:08	Broadcast	ARP	60 Who has 192.168.127.
16	5.245530182	192.168.127.138	1.1.1.1	IPv4	1514 Fragmented IP protocol

► Ethernet II, Src: Vmware\_e2:c5:bd (00:50:56:e2:c5:bd), Dst: Vmware\_fd:d5:80 (00:0c:29:fd:d5:80)  
 ▾ Address Resolution Protocol (reply)  
 Hardware type: Ethernet (1)  
 Protocol type: IPv4 (0x0800)  
 Hardware size: 6  
 Protocol size: 4  
 Opcode: reply (2)  
 Sender MAC address: Vmware\_e2:c5:bd (00:50:56:e2:c5:bd)  
 Sender IP address: 192.168.127.2  
 Target MAC address: Vmware\_fd:d5:80 (00:0c:29:fd:d5:80)  
 Target IP address: 192.168.127.138

- Bước 3:** Tìm đến gói tin đầu tiên có địa chỉ nguồn là địa chỉ IP của máy trạm mà chúng ta đã thiết lập ở trên, địa chỉ đích là 1.1.1.1

No.	Time	Source	Destination	Protocol	Length	Info
7	3.712293981	Vmware_c0:00:08	Broadcast	ARP	60 Who has 192.168.127.2? Tell	
8	4.243860886	Vmware_fd:d5:80	Broadcast	ARP	42 Who has 192.168.127.2? Tell	
9	4.244362212	Vmware_e2:c5:bd	Vmware_fd:d5:80	ARP	60 192.168.127.2 is at 00:50:56:e2:c5:bd	
10	4.244371101	192.168.127.138	1.1.1.1	IPv4	1514 Fragmented IP protocol (proto)	
11	4.244398655	192.168.127.138	1.1.1.1	ICMP	562 Echo (ping) request id=0x0	

► Internet Protocol Version 4, Src: 192.168.127.138, Dst: 1.1.1.1  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 ► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 1500  
 Identification: 0x801b (32795)  
 ▾ Flags: 0x2000, More fragments  
 0.... .... .... = Reserved bit: Not set  
 .0.... .... .... = Don't fragment: Not set  
 ..1.... .... .... = More fragments: Set  
 ...0 0000 0000 0000 = Fragment offset: 0  
 Time to live: 64  
 Protocol: ICMP (1)  
 Header checksum: 0x92d1 [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 192.168.127.138

Mở rộng phần tiêu đề, ta có một số thông tin quan trọng sau:

- Version (phiên bản): 4
- Header Length (kích thước tiêu đề): 20 byte
- Total Length (kích thước cả gói tin): 1500 byte

- Identification: 0x801b
  - Flags:
    - Don't fragment: gói tin được phép phân mảnh (giá trị là 0)
    - More fragments: còn các mảnh khác (giá trị là 1)
    - Fragment offset = 0 cho thấy đây là mảnh đầu tiên của một gói tin bị phân mảnh
  - Time to live: 64
- **Bước 4:** Chọn gói tin thứ hai có địa chỉ nguồn là địa chỉ IP của máy trạm mà chúng ta đã thiết lập ở trên, địa chỉ đích là 1.1.1.1

No.	Time	Source	Destination	Protocol	Length	Info
7	3.712293981	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.127.2? Tell
8	4.243860886	Vmware_fd:d5:80	Broadcast	ARP	42	Who has 192.168.127.2? Tell
9	4.244362212	Vmware_e2:c5:bd	Vmware_fd:d5:80	ARP	60	192.168.127.2 is at 00:50:5
*	10 4.244371101	192.168.127.138	1.1.1.1	IPv4	1514	Fragmented IP protocol (pro
	11 4.244398655	192.168.127.138	1.1.1.1	ICMP	562	Echo (ping) request id=0x0

▼ Internet Protocol Version 4, Src: 192.168.127.138, Dst: 1.1.1.1

```

    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 548
    Identification: 0x801b (32795)
    ▶ Flags: 0x000b9
        0.... .... .... = Reserved bit: Not set
        .0.... .... .... = Don't fragment: Not set
        ..0.... .... .... = More fragments: Not set
        ...0 0000 1011 1001 = Fragment offset: 185
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xb5d0 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.127.138
  
```

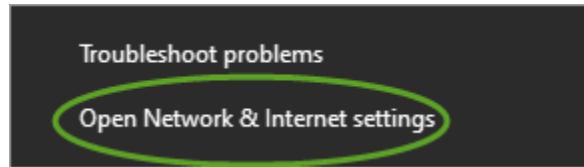
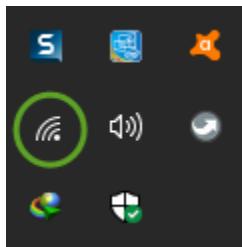
Mở rộng phần tiêu đề, ta có một số thông tin quan trọng tương tự gói tin trước. Chúng ta chú ý vào các trường sau:

- Identification: 0x801b trùng với gói trên. Như vậy đây là một mảnh cùng một gói tin với mảnh trên.
- Flags:
  - Don't fragment: gói tin được phép phân mảnh (giá trị là 0)
  - More fragments: không còn các mảnh khác (giá trị là 0)
  - Fragment offset = 185 cho thấy đây là mảnh tiếp theo

## 10.2. Phân tích hoạt động trên Windows

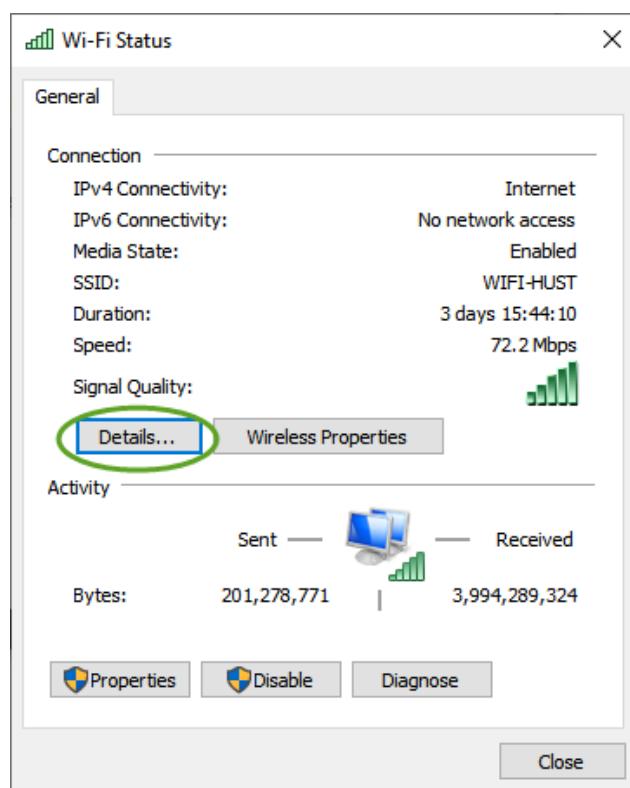
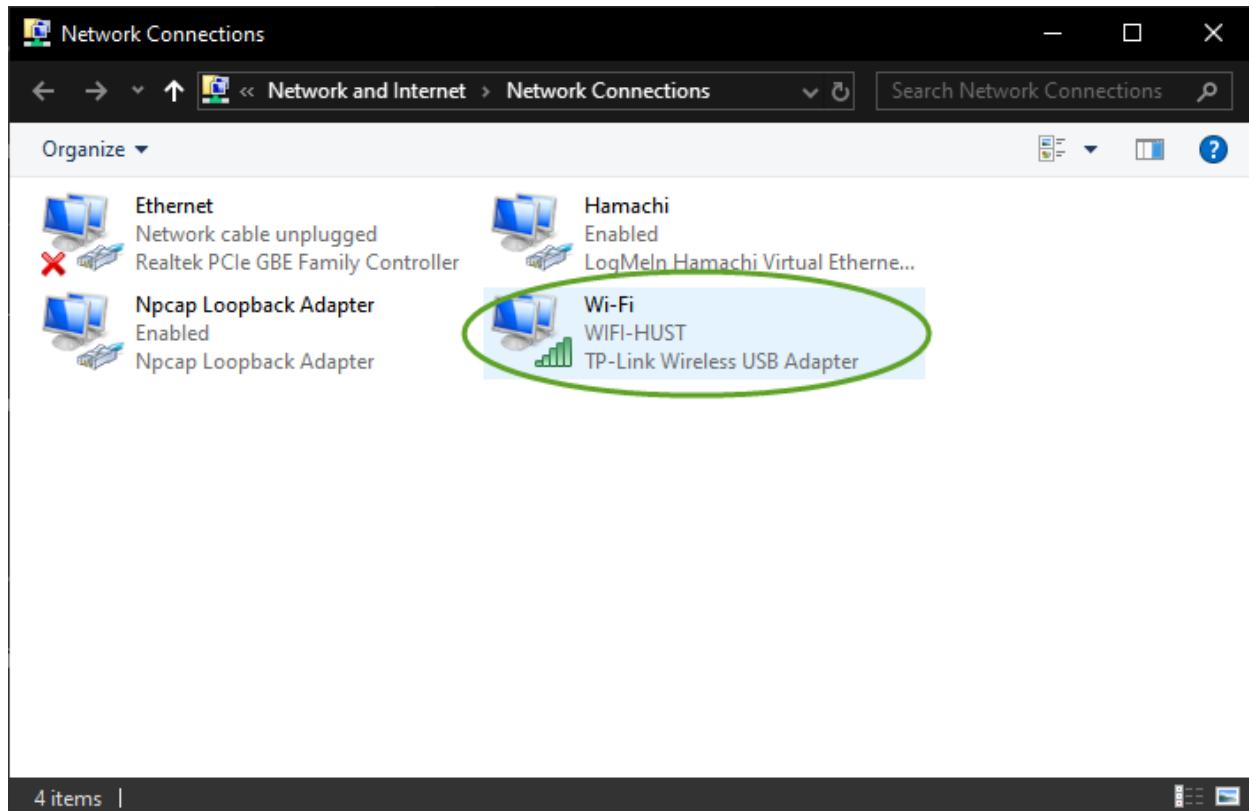
### 10.2.1. Cấu hình các thông số địa chỉ IP cho máy trạm

- **Bước 1 (vào phần cài đặt mạng):** Để không làm gián đoạn kết nối mạng của máy trạm, trước tiên ta tìm xem máy trạm đang sử dụng địa chỉ IP nào. Nhấn chuột phải biểu tượng kết nối mạng ở góc dưới bên phải của màn hình, chọn mục **Open Network & Internet settings**, ở cửa sổ mới chọn tiếp mục **Change adapter options**

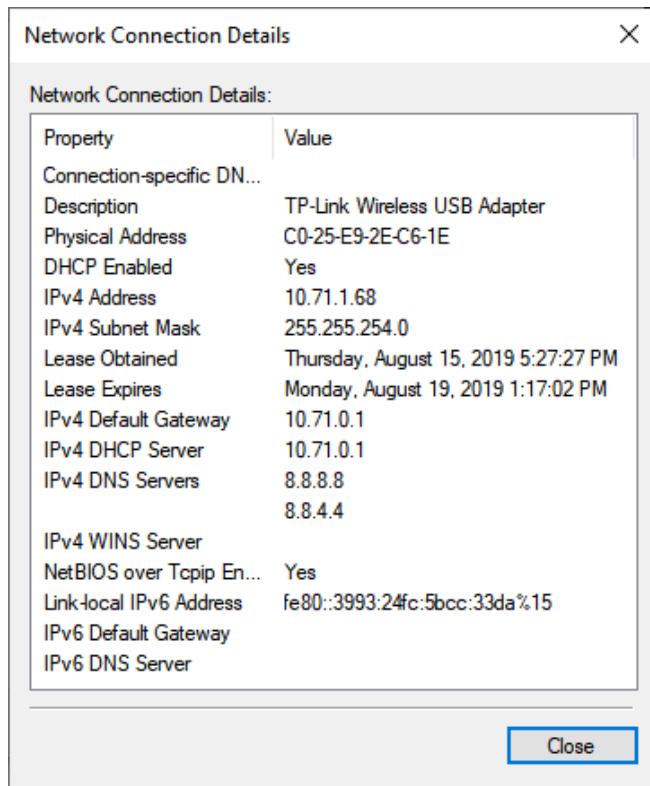


A screenshot of the Windows Network &amp; Internet settings page. On the left, there's a sidebar with options like Home, Find a setting, Network &amp; Internet, Status, Wi-Fi, Ethernet, Dial-up, VPN, Airplane mode, Mobile hotspot, Data usage, and Proxy. The "Status" section shows a connection to "WIFI-HUST" Public network. The "Change your network settings" section contains links for Change adapter options (which is circled in green), Sharing options, Network troubleshooter, View your network properties, and Windows Firewall.

- **Bước 2 (xem thông tin mạng – nếu có):** Nhấn đúp vào biểu tượng **Wi-Fi** mở cửa sổ **Wi-Fi Status**, chọn **Details**



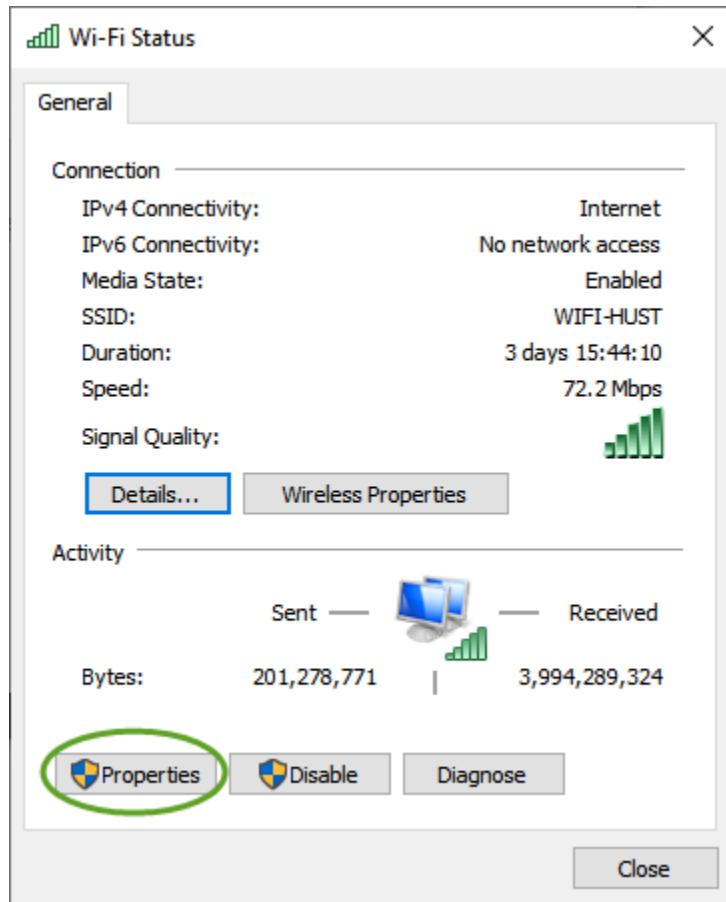
- **Bước 3 (thông tin kết nối mạng):** Chúng ta có thể thấy các thông số địa chỉ IP mà máy tính đang sử dụng. Ví dụ minh họa như hình dưới đây:

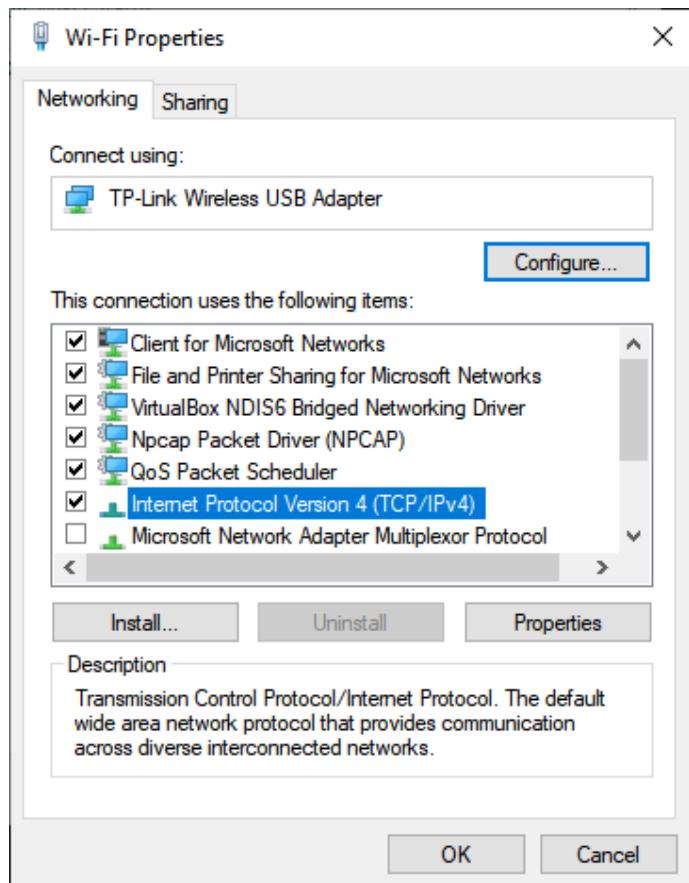


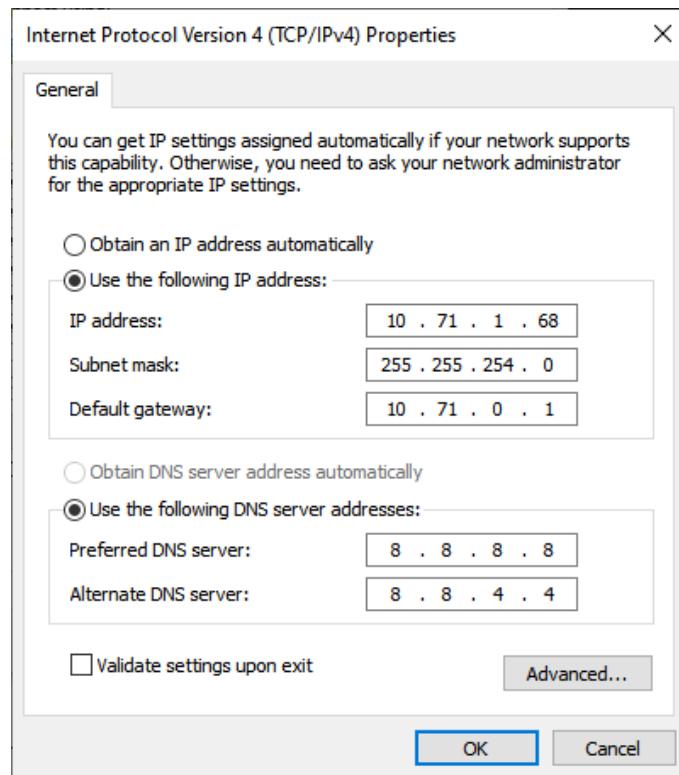
Các thông số này bao gồm:

- IP Address (Địa chỉ IP): 10.71.1.68. Địa chỉ này không kèm mặt nạ mạng nên có thể coi đó là địa chỉ phân lớp. Để thấy đây là địa chỉ phân lớp C nên có số bit mặc định của Network ID là 24.
- IPv4 Subnet Mask (Mặt nạ Mạng): 255.255.254.0
- IPv4 Default Gateway (Router mặc định): 10.71.0.1
- DNS (Địa chỉ máy chủ DNS): 8.8.8.8 – 8.8.4.4

- **Bước 4 (cấu hình IP bằng tay):** Chọn **Close** đóng cửa sổ hiện tại. Ở cửa sổ **Wi-Fi Status**, chọn **Properties** rồi chọn **Internet Protocol (TCP/IPv4)**. Chọn mục IPv4 của cửa sổ trên và điền các thông số mà chúng ta đã thấy ở bước trên như sau. Nhấn nút **OK** sau khi đã thiết lập xong.







**- Bước 5 (cấu hình mạng sau khi cài đặt):** Trên cửa sổ Command Prompt, chúng ta có thể sử dụng lệnh ipconfig /all để xem thông tin cấu hình địa chỉ IP của máy trạm:

```
C:\WINDOWS\system32\cmd.exe
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . :
  Description . . . . . : TP-Link Wireless USB Adapter
  Physical Address. . . . . : C0-25-E9-2E-C6-1E
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::3993:24fc:5bcc:33da%15(PREFERRED)
  IPv4 Address. . . . . : 10.71.1.68(Preferred)
  Subnet Mask . . . . . : 255.255.254.0
  Lease Obtained. . . . . : Thursday, August 15, 2019 5:27:27 PM
  Lease Expires . . . . . : Saturday, August 17, 2019 6:10:34 PM
  Default Gateway . . . . . : 10.71.0.1
  DHCP Server . . . . . : 10.71.0.1
  DHCPv6 IAID . . . . . : 79701481
  DHCPv6 Client DUID . . . . . : 00-01-00-01-21-5A-8B-45-48-4D-7E-EA-C2-0A
  DNS Servers . . . . . : 8.8.8.8
                                8.8.4.4
  NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Hamachi:
  Connection-specific DNS Suffix . :
  Description . . . . . : LogMeIn Hamachi Virtual Ethernet Adapter
  Physical Address. . . . . : 02-50-F2-65-32-00
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Default Gateway . . . . . : 25.0.0.1
```

- **Bước 6 (kiểm thử):** Chúng ta có thể truy cập vào website bất kỳ để kiểm chứng các thiết lập trên là chính xác hay không.

### 10.2.2. Sử dụng Wireshark để bắt gói tin

- **Bước 1:** Mở Windows Explorer vào đường dẫn cài đặt, khởi động Wireshark (ví dụ đường dẫn mặc định là: C:\Program Files\Wireshark\Wireshark.exe).
- **Bước 2:** Bắt đầu bắt gói tin trên các mạng phù hợp với Wireshark.
- **Bước 3:** Mở cửa sổ Command Prompt với quyền quản trị Administrator và gõ lệnh sau để xóa bảng ARP Table của máy trạm:

```
C:\WINDOWS\system32>netsh interface ip delete arpcach
ok.
```

- **Bước 5:** Trên cửa sổ Command Prompt thực hiện lệnh ping 1.1.1.1 -s 4 -c 4 như sau:

```
C:\Users\ttmlab>ping 1.1.1.1 -s 4 -n 4
```

Khi lệnh này thực hiện xong, dừng bắt gói tin. Trên cửa sổ của Wireshark, chúng ta sẽ thấy các gói tin tương tự như sau:

No.	Time	Source	Destination	Protocol	Length	Info
11	0.035496	204.79.197.200	10.71.1.68	TLSv1.2	109	Application Data
12	0.035578	10.71.1.68	204.79.197.200	TCP	54	65126 → 443 [ACK] Seq=3973 Ack=111 Win=1023 Len=0
13	0.987728	204.79.197.200	10.71.1.68	TLSv1.2	196	Application Data
14	0.987802	10.71.1.68	204.79.197.200	TCP	54	65126 → 443 [ACK] Seq=3973 Ack=253 Win=1023 Len=0
15	5.341103	10.71.1.68	1.1.1.1	ICMP	114	Echo (ping) request id=0x0001, seq=281/6401, ttl=64
16	5.369794	1.1.1.1	10.71.1.68	ICMP	114	Echo (ping) reply id=0x0001, seq=281/6401, ttl=64
17	5.492336	10.71.1.68	40.90.189.152	TCP	55	64907 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a retransmission]
18	5.540772	40.90.189.152	10.71.1.68	TCP	66	443 → 64907 [ACK] Seq=1 Ack=2 Win=7001 Len=0 SLE=1

> Frame 1: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface 0  
 > Ethernet II, Src: Tp-LinkT\_2e:c6:1e (c0:25:e9:2e:c6:1e), Dst: Routerbo\_31:f6:e8 (e4:8d:8c:31:f6:e8)  
 > Internet Protocol Version 4, Src: 10.71.1.68, Dst: 204.79.197.200  
 > Transmission Control Protocol, Src Port: 65126, Dst Port: 443, Seq: 1, Ack: 1, Len: 507  
 > Transport Layer Security

0000 e4 8d 8c 31 f6 e8 c0 25 e9 2e c6 1e 08 00 45 00 . . . . . . . . . . . . E .  
 0010 02 23 49 2c 40 00 80 06 12 06 0a 47 01 44 cc 4f #I, @ . . . . G . D . O  
 0020 c5 c8 fe 66 01 bb 43 84 67 ec fe 95 e5 d8 50 18 . . . f . C . g . . . . P .  
 0030 04 00 63 ec 00 00 17 03 03 01 f6 00 00 00 00 00 . . . c . . . . . . . . . . .  
 0040 00 00 1f 63 b8 a2 c8 14 8f 33 33 32 fe ea 42 54 . . . c . . . . 332 . . B T

Ready to load or capture || Packets: 26 · Displayed: 26 (100.0%) || Profile: Default

- **Bước 6:** Mở cửa sổ Command Prompt thứ hai, sử dụng lệnh **arp -a** để xem thông tin bảng ARP Table.

```
C:\Users\ttm\lab>arp -a

Interface: 10.71.1.68 --- 0xf
Internet Address      Physical Address      Type
10.71.0.1            e4-8d-8c-31-f6-e8    dynamic
10.71.1.255          ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250     01-00-5e-7f-ff-fa    static
255.255.255.255     ff-ff-ff-ff-ff-ff    static

Interface: 169.254.181.112 --- 0x3b
Internet Address      Physical Address      Type
169.254.255.255     ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250     01-00-5e-7f-ff-fa    static
255.255.255.255     ff-ff-ff-ff-ff-ff    static
```

#### **Lưu ý:**

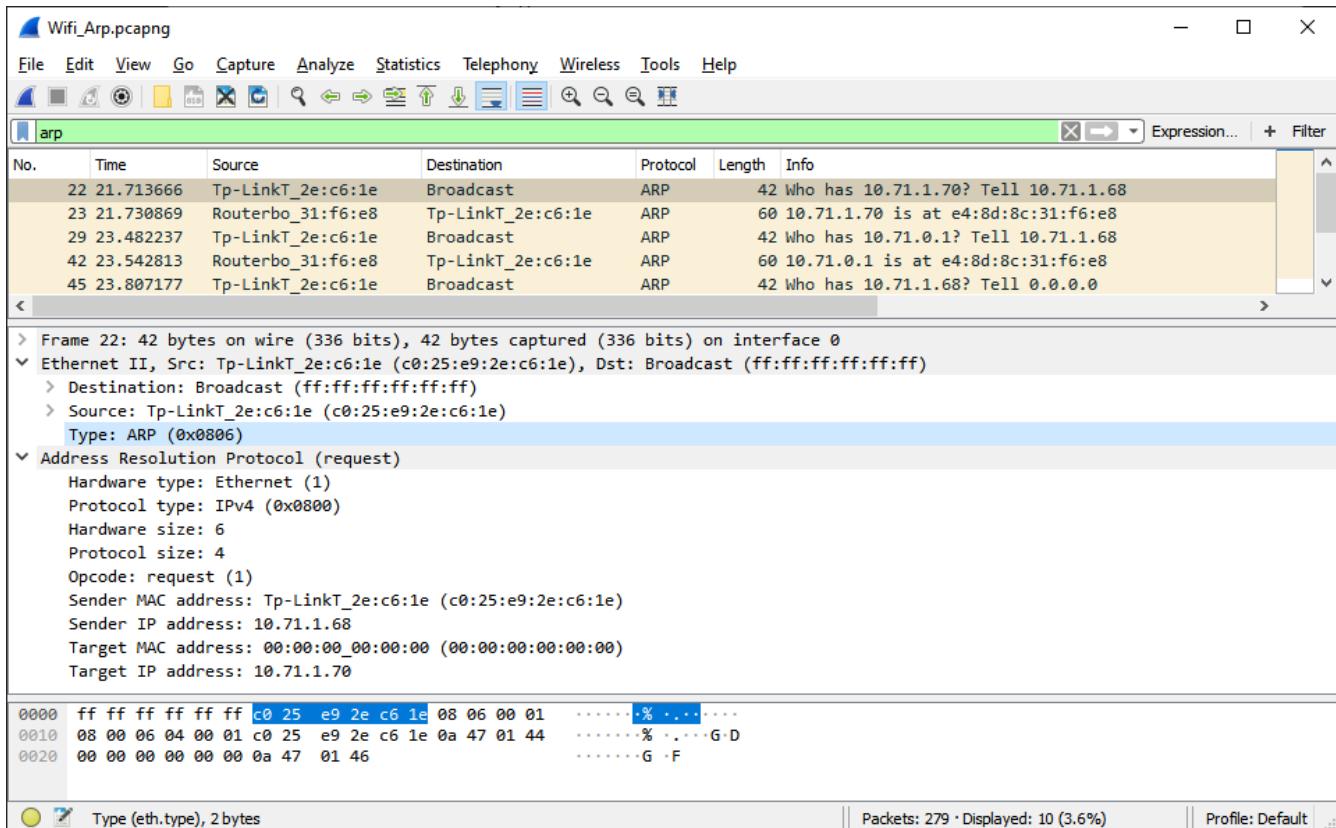
- Nếu trên máy học viên không bắt được các gói tin có Protocol là ARP thì nên thực hiện lại từ bước 1.
- Các gói tin bắt được trên máy các bạn có thể sẽ có thông số khác. Điều này là hoàn toàn bình thường và không có ảnh hưởng tới quá trình thực hành.

#### **10.2.3. Phân tích lưu lượng**

*Lưu ý: Các giá trị phân tích dưới đây chỉ mang tính chất minh họa. Với lưu lượng bắt trên máy sinh viên, kết quả có thể sẽ khác. Các bạn có thể download file lưu lượng mẫu tại địa chỉ sau cho nội dung minh họa dưới đây:*

<https://drive.google.com/file/d/1iFg6Y3sk5fS1tC3FdtGHPVPlQhfI3y4Z>

- **Bước 1:** Bạn có thể thấy trên file lưu lượng bắt được một số gói tin có Protocol là ARP và địa chỉ nguồn là địa chỉ máy của bạn. Mở rộng phần tiêu đề **Address Resolution Protocol**, chúng ta có thể thấy đây là gói tin ARP Request.



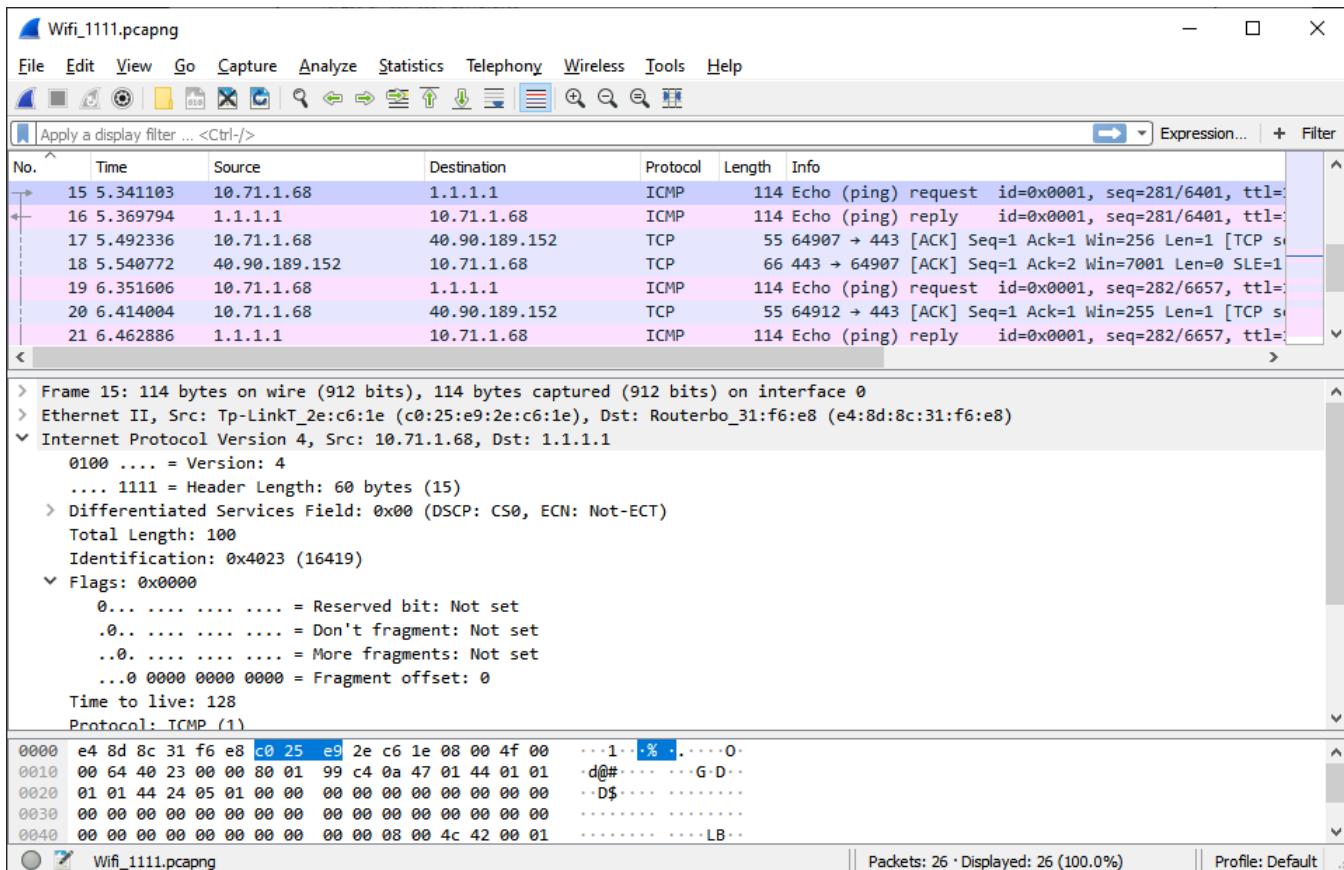
Các thông tin chúng ta đọc được từ phần tiêu đề này gồm có:

- Hardware type: Chuẩn phần cứng sử dụng trong ví dụ này là Ethernet.
- Protocol type: giao thức là IPv4.
- Hardware size: kích thước phần cứng là 6 byte (địa chỉ MAC).
- Protocol size: địa chỉ giao thức tầng trên là 4 byte.
- Sender MAC address: địa chỉ MAC nút nguồn.
- Sender IP address: địa chỉ IP của nút nguồn.
- Target MAC address: địa chỉ MAC cần tìm kiếm.
- Target IP address: địa chỉ IP đã biết.

- **Bước 2:** Tiếp theo, bạn sẽ thấy gói tin trả lời là gói tin ARP có địa chỉ đích là địa chỉ MAC máy tính của bạn. Các thông tin trong gói này tương tự ở trên, với điểm khác biệt là địa chỉ Target MAC address đã là địa chỉ cần tìm kiếm. Các bạn có thể thấy rằng, đây cũng chỉ là địa chỉ nguồn của khung tin Ethernet mang theo gói ARP Reply trả lời.



- **Bước 3:** Tìm đến gói tin đầu tiên có địa chỉ nguồn là địa chỉ IP của máy trạm mà chúng ta đã thiết lập ở trên, địa chỉ đích là 1.1.1.1



Mở rộng phần tiêu đề, ta có một số thông tin quan trọng sau:

- Version (phiên bản): 4
- Header Length (kích thước tiêu đề): 60 byte
- Total Length (kích thước cả gói tin): 100 byte
- Identification: 0x4023
- Flags:
  - Don't fragment: gói tin được phép phân mảnh (giá trị là 0)
  - More fragments: còn các mảnh khác (giá trị là 0)
  - Fragment offset = 0 cho thấy đây là mảnh đầu tiên của một gói tin bị phân mảnh
- Time to live: 128

- **Bước 4:** Chọn gói tin thứ hai có địa chỉ nguồn là địa chỉ IP của máy trạm mà chúng ta đã thiết lập ở trên, địa chỉ đích là 1.1.1.1

No.	Time	Source	Destination	Protocol	Length	Info
7	3.712293981	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.127.2? Tell
8	4.243860886	Vmware_fd:d5:80	Broadcast	ARP	42	Who has 192.168.127.2? Tell
9	4.244362212	Vmware_e2:c5:bd	Vmware_fd:d5:80	ARP	60	192.168.127.2 is at 00:50:5
• 10	4.244371101	192.168.127.138	1.1.1.1	IPv4	1514	Fragmented IP protocol (pro
↑ 11	4.244398655	192.168.127.138	1.1.1.1	ICMP	562	Echo (ping) request id=0x0

Internet Protocol Version 4, Src: 192.168.127.138, Dst: 1.1.1.1  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 548  
 Identification: 0x801b (32795)  
 ▶ Flags: 0x00b9  
 0.... .... .... = Reserved bit: Not set  
 .0.... .... .... = Don't fragment: Not set  
 ..0.... .... .... = More fragments: Not set  
 ...0 0000 1011 1001 = Fragment offset: 185  
 Time to live: 64  
 Protocol: ICMP (1)  
 Header checksum: 0xb5d0 [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 192.168.127.138

Mở rộng phần tiêu đề, ta có một số thông tin quan trọng tương tự gói tin trước. Chúng ta chú ý vào các trường sau:

- Identification: 0x801b trùng với gói trên. Như vậy đây là một mảnh cùng một gói tin với mảnh trên.
- Flags:
  - Don't fragment: gói tin được phép phân mảnh (giá trị là 0)
  - More fragments: không còn các mảnh khác (giá trị là 0)
  - Fragment offset = 185 cho thấy đây là mảnh tiếp theo

## 7. PHỤ LỤC 4: KIỂM TRA TÌNH TRẠNG KẾT NỐI

### 11.1 Kiểm tra tình trạng kết nối trên Ubuntu

#### 11.1.1. Sử dụng công cụ ping

Lưu ý: Những hình ảnh dưới đây mang tính chất ví dụ minh họa. Kết quả thực hiện trên máy sinh viên có thể sẽ khác.

- **Bước 1:** Mở Wireshark bằng lệnh **sudo wireshark** trên cửa sổ Terminal thứ nhất
- **Bước 2:** Trên cửa sổ Terminal thứ hai thực hiện lệnh ping như dưới đây:

```
student@ubuntu:~$ ping google.com -c 5
PING google.com (216.58.203.46) 56(84) bytes of data.
64 bytes from hkg12s10-in-f46.1e100.net (216.58.203.46): icmp_seq=1 ttl=128 time=61.9 ms
64 bytes from hkg12s10-in-f46.1e100.net (216.58.203.46): icmp_seq=2 ttl=128 time=61.7 ms
64 bytes from hkg12s10-in-f46.1e100.net (216.58.203.46): icmp_seq=3 ttl=128 time=62.1 ms
64 bytes from hkg12s10-in-f46.1e100.net (216.58.203.46): icmp_seq=4 ttl=128 time=61.9 ms
64 bytes from hkg12s10-in-f46.1e100.net (216.58.203.46): icmp_seq=5 ttl=128 time=61.9 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 61.747/61.950/62.145/0.202 ms
```

- Bước 3: Sau khi lệnh ping ở trên kết thúc, thực hiện lệnh ping lần 2 như sau:

```
student@ubuntu:~$ ping 1.2.3.4 -c 5
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.

--- 1.2.3.4 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4073ms
```

- Bước 4: Ngừng bắt gói tin trên Wireshark
- Bước 5: Trên Wireshark điền xâu icmp vào bộ lọc để lọc lấy các gói tin ICMP. Kết quả nhận được sẽ tương tự như sau:

No.	Time	Source	Destination	Protocol	Length	Info
5	0.056861561	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request id=0x2f67, seq=1/256, ttl=64 (rep)
6	0.118810868	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply id=0x2f67, seq=1/256, ttl=128 (req)
9	1.058983563	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request id=0x2f67, seq=2/512, ttl=64 (rep)
10	1.120684815	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply id=0x2f67, seq=2/512, ttl=128 (req)
11	2.061669915	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request id=0x2f67, seq=3/768, ttl=64 (rep)
12	2.123765867	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply id=0x2f67, seq=3/768, ttl=128 (req)
15	3.063778239	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request id=0x2f67, seq=4/1024, ttl=64 (rep)
16	3.125695987	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply id=0x2f67, seq=4/1024, ttl=128 (req)
17	4.065286510	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request id=0x2f67, seq=5/1280, ttl=64 (rep)
18	4.127182217	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply id=0x2f67, seq=5/1280, ttl=128 (req)
19	13.568264440	192.168.127.138	1.2.3.4	ICMP	98	Echo (ping) request id=0x2f68, seq=1/256, ttl=64 (no r)
20	14.569483954	192.168.127.138	1.2.3.4	ICMP	98	Echo (ping) request id=0x2f68, seq=2/512, ttl=64 (no r)
21	15.592572177	192.168.127.138	1.2.3.4	ICMP	98	Echo (ping) request id=0x2f68, seq=3/768, ttl=64 (no r)
22	16.617210863	192.168.127.138	1.2.3.4	ICMP	98	Echo (ping) request id=0x2f68, seq=4/1024, ttl=64 (no r)
23	17.614482460	192.168.127.138	1.2.3.4	ICMP	98	Echo (ping) request id=0x2f68, seq=5/1280, ttl=64 (no r)

### Phân tích kết quả:

- Kết quả của lệnh ping ở bước 2 cho thấy kết nối tới máy chủ google.com là bình thường. Từ kết quả này, ta còn thu được một số thông tin sau:

- Địa chỉ IP của máy chủ google.com: 216.58.203.46
- Tên khác của máy chủ: hkg12s10-in-f46.1e100.net
- Kích thước mỗi gói tin: 64 byte
- Số gói gửi: 5; số gói nhận: 5; tỉ lệ mất gói tin (packet loss): 0%
- (Trễ nhỏ nhất/trung bình/lớn nhất/độ lệch)rtt min/avg/max/mdev = 61.747/61.950/62.145/0.202 ms
- Thời gian thực hiện lệnh (time): 4008 ms

- Kết quả của lệnh ping ở bước 3 cho thấy kết nối tới máy có địa chỉ 1.2.3.4 là có lỗi, khi có 5 gửi đi thăm dò nhưng không nhận được gói trả lời nào (tỉ lệ mất gói tin là 100%)
- Mở rộng phần tiêu đề của gói tin Echo (ping) request bất kỳ ta thấy trường Type là 8 cho thấy gói tin là ICMP Echo Request

No.	Time	Source	Destination	Protocol	Length	Info
5	0.056861561	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request
6	0.118810868	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply
9	1.058983563	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request
10	1.120684815	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply
11	2.061669915	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request
12	2.123765867	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply
15	3.063778239	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request
16	3.125695987	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply
17	4.065286510	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request
18	4.127182217	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply
19	4.127182217	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request

▶ Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
 ▶ Ethernet II, Src: VMware\_fd:d5:80 (00:0c:29:fd:d5:80), Dst: VMware\_e2:c5:bd (00:50:56:e2:c5:bd)  
 ▶ Internet Protocol Version 4, Src: 192.168.127.138, Dst: 216.58.203.46  
 ▶ Internet Control Message Protocol  
 Type: 8 (Echo (ping) request)  
 Code: 0  
 Checksum: 0xb28d [correct]  
 [Checksum Status: Good]  
 Identifier (BE): 12135 (0x2f67)  
 Identifier (LE): 26415 (0x672f)  
 Sequence number (BE): 1 (0x0001)  
 Sequence number (LE): 256 (0x0100)  
 [Response frame: 6]  
 Timestamp from icmp data: Aug 21, 2018 09:12:58.000000000 PDT  
 [Timestamp from icmp data (relative): 0.434656836 seconds]  
 ▶ Data (48 bytes)  
 Data: caa1060000000000101112131415161718191a1b1c1d1e1f...  
 [Length: 48]

- Mở rộng phần tiêu đề của gói tin Echo (ping) reply của gói trên ta thấy trường Type là 0 cho thấy gói tin này là ICMP Echo Reply. Hơn nữa, ta có thể thấy nội dung phần Data(48 bytes) giống với gói tin ICMP Echo Request ở trên

No.	Time	Source	Destination	Protocol	Length	Info
5	0.056861561	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request
6	0.118810868	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply
9	1.058983563	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request
10	1.120684815	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply
11	2.061669915	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request
12	2.123765867	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply
15	3.063778239	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request
16	3.125695987	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply
17	4.065286510	192.168.127.138	216.58.203.46	ICMP	98	Echo (ping) request
18	4.127102217	216.58.203.46	192.168.127.138	ICMP	98	Echo (ping) reply

▶ Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
 ▶ Ethernet II, Src: VMware\_e2:c5:bd (00:50:56:e2:c5:bd), Dst: VMware\_fd:d5:80 (00:0c:29:fd:d5:80)  
 ▶ Internet Protocol Version 4, Src: 216.58.203.46, Dst: 192.168.127.138  
 ▶ Internet Control Message Protocol  
 Type: 0 (Echo (ping) reply)  
 Code: 0  
 Checksum: 0xba8d [correct]  
 [Checksum Status: Good]  
 Identifier (BE): 12135 (0x2f67)  
 Identifier (LE): 26415 (0x672f)  
 Sequence number (BE): 1 (0x0001)  
 Sequence number (LE): 256 (0x0100)  
 [Request frame: 5]  
 [Response time: 61.949 ms]  
 Timestamp from icmp data: Aug 21, 2018 09:12:58.000000000 PDT  
 [Timestamp from icmp data (relative): 0.496606143 seconds]  
 ▶ Data (48 bytes)  
 Data: caa10600000000000101112131415161718191a1b1c1d1e1f...  
 [Length: 48]

### 11.1.2. Sử dụng công cụ traceroute

Công cụ traceroute đã được cài đặt mặc định trên Ubuntu 18.04, nhưng vì một lý do nào đó không có công cụ này, bạn có thể cài đặt bằng lệnh đơn giản sau trước khi thực hiện nội dung thực hành này:

**sudo apt-get install traceroute**

- Bước 1:** Mở Wireshark bằng lệnh trên cửa sổ Terminal thứ nhất
- Bước 2:** Trên cửa sổ Terminal thứ hai thực hiện lệnh traceroute như dưới đây:

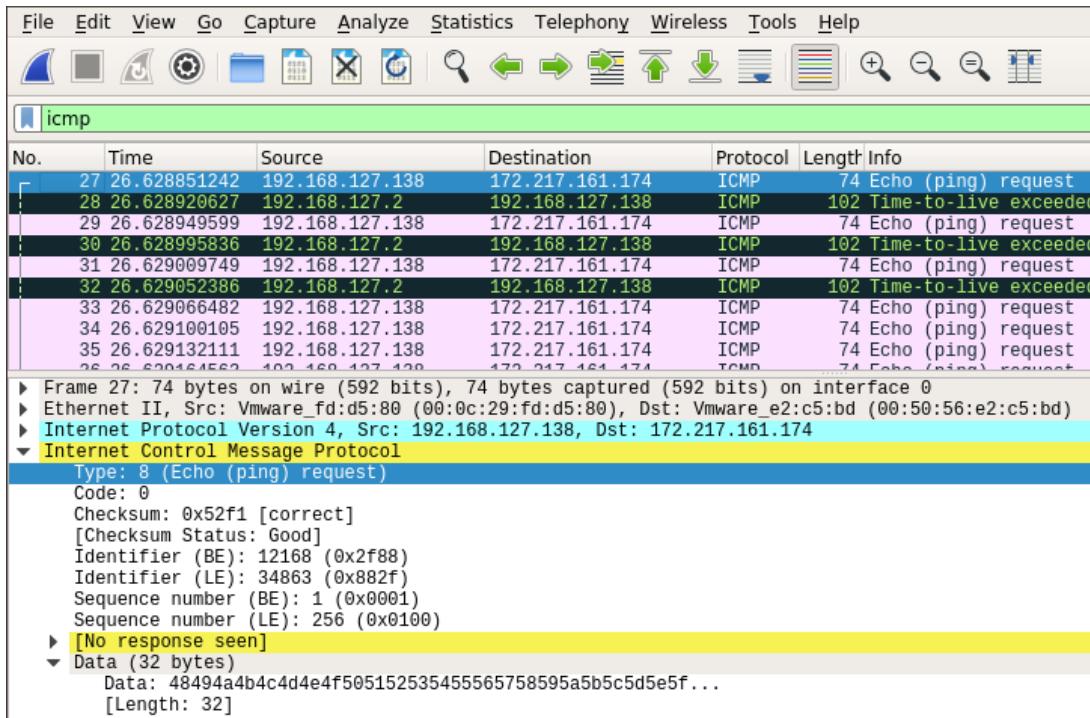
```
student@ubuntu:~$ sudo traceroute google.com -I
traceroute to google.com (216.58.200.14), 30 hops max, 60 byte packets
 1 _gateway (192.168.127.2)  0.171 ms  0.166 ms  0.152 ms
 2 192.168.1.1 (192.168.1.1)  2.891 ms static.vnpt-hanoi.com.vn (123.25.17.65)  12.297 ms static.vnpt.vn (14.177.176.25
 4) 8.443 ms
 3 static.vnpt.vn (14.177.176.254)  7.800 ms static.vnpt-hanoi.com.vn (123.25.17.65)  10.463 ms  10.267 ms
 4 static.vnpt-hanoi.com.vn (123.25.17.65)  14.498 ms  13.826 ms static.vnpt.vn (113.171.34.157)  16.305 ms
 5 static.vnpt.vn (113.171.34.157)  16.950 ms  17.345 ms static.vnpt.vn (113.171.35.157)  18.215 ms
 6 static.vnpt.vn (113.171.35.157)  21.709 ms static.vnpt.vn (113.171.5.114)  8.180 ms  6.140 ms
 7 static.vnpt.vn (113.171.5.114)  9.991 ms 72.14.242.32 (72.14.242.32)  30.649 ms  28.583 ms
 8 72.14.242.32 (72.14.242.32)  32.469 ms 108.170.241.97 (108.170.241.97)  35.237 ms  34.160 ms
 9 108.170.241.97 (108.170.241.97)  36.817 ms  37.946 ms  38.114 ms
10 209.85.240.11 (209.85.240.11)  48.129 ms 48.478 ms hkg12s11-in-f14.1.e100.net (216.58.200.14)  49.187 ms
```

Lưu ý: Với tùy chọn **-I** lệnh này sẽ gửi đi các gói tin ICMP Echo Request thay vì dùng các gói tin UDP theo mặc định

- Bước 3:** Sau khi lệnh traceroute ở trên kết thúc, thực hiện lệnh traceroute lần 2 như sau:

```
student@ubuntu:~$ sudo traceroute 1.2.3.4 -I
traceroute to 1.2.3.4 (1.2.3.4), 30 hops max, 60 byte packets
 1 _gateway (192.168.127.2)  0.267 ms  0.143 ms  0.094 ms
 2 192.168.1.1 (192.168.1.1)  4.771 ms static.vnpt.vn (14.177.176.254)  10.685 ms  12.111 ms
 3 static.vnpt.vn (14.177.176.254)  8.321 ms  12.995 ms static.vnpt-hanoi.com.vn (123.25.17.65)  14.116 ms
 4 static.vnpt-hanoi.com.vn (123.25.17.65)  16.221 ms * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
```

- **Bước 4:** Ngừng bắt gói tin trên Wireshark
- **Bước 5:** Trên Wireshark điền xâu icmp vào bộ lọc để lọc lấy các gói tin ICMP. Kết quả nhận được sẽ tương tự như sau:



### Phân tích kết quả:

- Kết quả của lệnh traceroute ở bước 2 cho thấy từ máy tính thực hiện tới máy chủ google.com có 10 chặng đi qua với địa chỉ IP của mỗi chặng đã được liệt kê.
- Kết quả của lệnh traceroute ở bước 3 cho thấy bắt đầu từ chặng thứ 5, lệnh này không phân tích được địa chỉ. Như vậy, có thể phán đoán, kết nối của máy tính thực hiện lệnh tới máy 1.2.3.4 bắt đầu có lỗi từ bước này.
- Trên kết quả bắt gói tin của Wireshark, chúng ta có thể thấy các nhóm 3 gói tin ICMP được gửi đi. Sau khi gửi xong một nhóm, giá trị TTL của nhóm tiếp theo tăng thêm 1.

Địa chỉ nguồn của các gói tin báo lỗi ICMP Time to live exceeded chính là địa chỉ các chặng.

No.	Time	Source	Destination	Protocol	Length	Info
5	0.055960594	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=1/256, ttl=1 (Time to live exceeded)
6	0.056030973	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=2/512, ttl=1 (Time to live exceeded)
7	0.056064816	192.168.127.2	192.168.127.138	ICMP	102	Time-to-live exceeded (Time to live exceeded in tra
8	0.056099846	192.168.127.2	192.168.127.138	ICMP	102	Time-to-live exceeded (Time to live exceeded in tra
9	0.0561113695	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=3/768, ttl=1 (Time to live exceeded)
10	0.056148893	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=4/1024, ttl=2 (Time to live exceeded)
11	0.056178858	192.168.127.2	192.168.127.138	ICMP	102	Time-to-live exceeded (Time to live exceeded in tra
12	0.056191398	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=5/1280, ttl=2 (Time to live exceeded)
13	0.056223474	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=6/1536, ttl=2 (Time to live exceeded)
14	0.056255932	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=7/1792, ttl=3 (Time to live exceeded)
15	0.056332884	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=8/2048, ttl=3 (Time to live exceeded)
16	0.056408276	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=9/2304, ttl=3 (Time to live exceeded)
17	0.056455698	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=10/2560, ttl=4 (Time to live exceeded)
18	0.056487894	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=11/2816, ttl=4 (Time to live exceeded)
19	0.056532239	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=12/3072, ttl=4 (Time to live exceeded)
20	0.056564896	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=13/3328, ttl=5 (Time to live exceeded)
21	0.056615717	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=14/3584, ttl=5 (Time to live exceeded)
22	0.056683615	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=15/3840, ttl=5 (Time to live exceeded)
23	0.056730465	192.168.127.138	172.217.24.206	ICMP	74	Echo (ping) request id=0x2fa1, seq=16/4096, ttl=6 (Time to live exceeded)
25	0.061724034	14.177.176.254	192.168.127.138	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
26	0.063809129	14.177.176.254	192.168.127.138	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
27	0.065558768	14.177.176.254	192.168.127.138	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
28	0.067116817	123.25.17.65	192.168.127.138	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
29	0.068781275	123.25.17.65	192.168.127.138	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
30	0.070757695	123.25.17.65	192.168.127.138	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
31	0.071768596	113.171.34.157	192.168.127.138	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
32	0.072738908	113.171.34.157	192.168.127.138	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
33	0.073282377	113.171.34.157	192.168.127.138	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra

## 11.2 Kiểm tra tình trạng kết nối trên Windows

### 11.2.1. Sử dụng công cụ ping

Lưu ý: Những hình ảnh dưới đây mang tính chất ví dụ minh họa. Kết quả thực hiện trên máy sinh viên có thể sẽ khác.

- Bước 1:** Mở Windows Explorer vào đường dẫn cài đặt, khởi động Wireshark (ví dụ đường dẫn mặc định là: C:\Program Files\Wireshark\Wireshark.exe).
- Bước 2:** Mở Command Prompt thực hiện lệnh ping như dưới đây:

```
C:\Users\ttmlab>ping google.com -n 5

Pinging google.com [172.217.24.206] with 32 bytes of data:
Reply from 172.217.24.206: bytes=32 time=24ms TTL=51
Reply from 172.217.24.206: bytes=32 time=28ms TTL=51
Reply from 172.217.24.206: bytes=32 time=27ms TTL=51
Reply from 172.217.24.206: bytes=32 time=26ms TTL=51
Reply from 172.217.24.206: bytes=32 time=50ms TTL=51

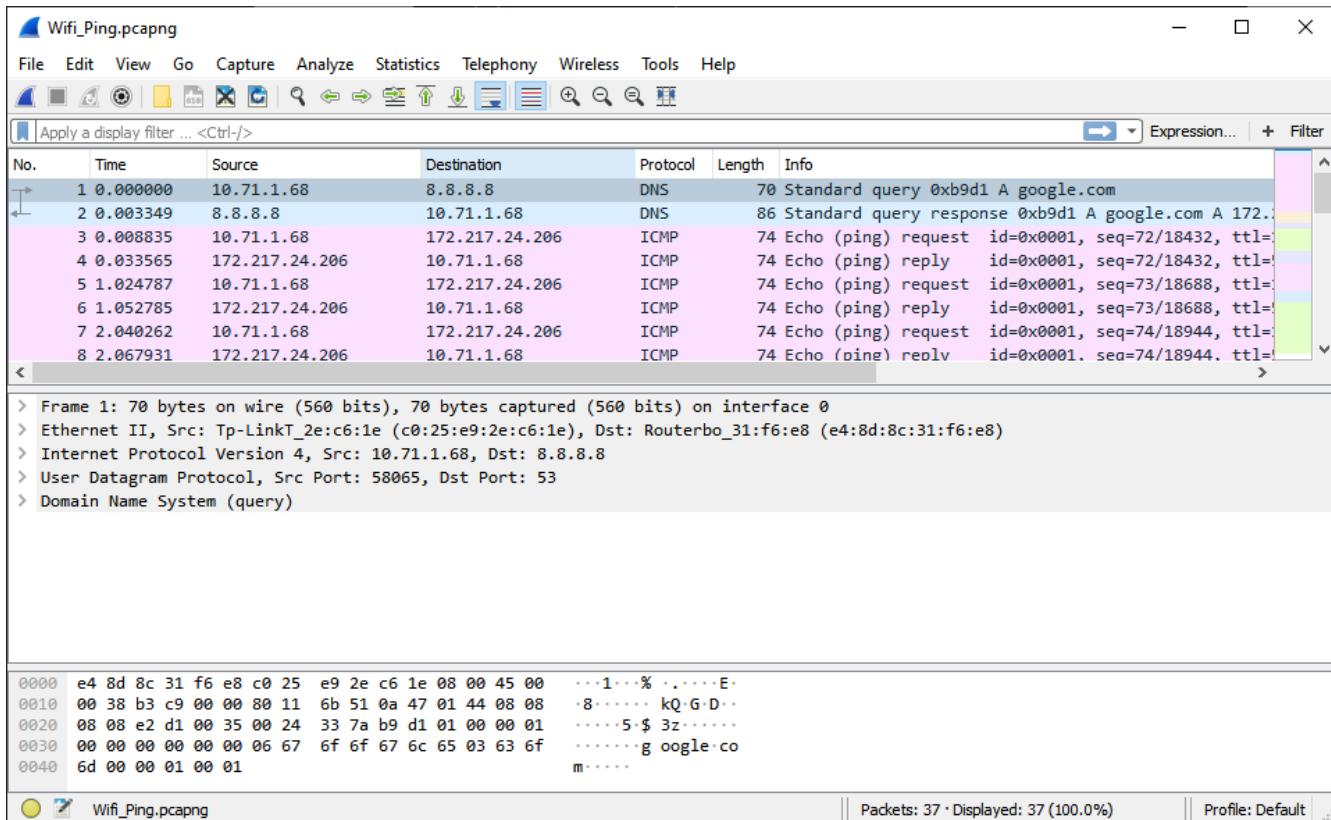
Ping statistics for 172.217.24.206:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 50ms, Average = 31ms
```

- Bước 3:** Sau khi lệnh ping ở trên kết thúc, thực hiện lệnh ping lần 2 như sau:

```
C:\Users\ttm\lab>ping 1.2.3.4 -n 5
Pinging 1.2.3.4 with 32 bytes of data:
Request timed out.

Ping statistics for 1.2.3.4:
  Packets: Sent = 5, Received = 0, Lost = 5 (100% loss),
```

- **Bước 4:** Ngừng bắt gói tin trên Wireshark
- **Bước 5:** Trên Wireshark điền xâu icmp vào bộ lọc để lọc lấy các gói tin ICMP. Kết quả nhận được sẽ tương tự như sau:



### Phân tích kết quả:

- Kết quả của lệnh ping ở bước 2 cho thấy kết nối tới máy chủ google.com là bình thường. Từ kết quả này, ta còn thu được một số thông tin sau:

- Địa chỉ IP của máy chủ google.com: 172.217.24.206
- **Tên khác của máy chủ: hkg12s10-in-f46.1e100.net**
- Kích thước mỗi gói tin: 32 bytes

- Số gói gửi: 5; số gói nhận: 5; tỉ lệ mất gói tin: 0%
  - Thời gian khứ hồi gần đúng tính bằng mili giây
- Nhỏ nhất = 24ms, Lớn nhất = 50ms, Trung bình = 31ms =  
 (Approximate round trip times in milli-seconds:  
 Minimum = 24ms, Maximum = 50ms, Average = 31ms)

- Thời gian thực hiện lệnh (time): 4008 ms

- Kết quả của lệnh ping ở bước 3 cho thấy kết nối tới máy có địa chỉ 1.2.3.4 là có lỗi, khi có 5 gửi đi thăm dò nhưng không nhận được gói trả lời nào (tỉ lệ mất gói tin là 100%)
- Mở rộng phần tiêu đề của gói tin Echo (ping) request bất kỳ ta thấy trường Type là 8 cho thấy gói tin là ICMP Echo Request

No.	Time	Source	Destination	Protocol	Length	Info
7	2.040262	10.71.1.68	172.217.24.206	ICMP	74	Echo (ping) request id=0x0001, seq=74/18944, ttl=
8	2.067931	172.217.24.206	10.71.1.68	ICMP	74	Echo (ping) reply id=0x0001, seq=74/18944, ttl=
9	3.055779	10.71.1.68	172.217.24.206	ICMP	74	Echo (ping) request id=0x0001, seq=75/19200, ttl=
10	3.082392	172.217.24.206	10.71.1.68	ICMP	74	Echo (ping) reply id=0x0001, seq=75/19200, ttl=
11	4.070882	10.71.1.68	172.217.24.206	ICMP	74	Echo (ping) request id=0x0001, seq=76/19456, ttl=
12	4.121663	172.217.24.206	10.71.1.68	ICMP	74	Echo (ping) reply id=0x0001, seq=76/19456, ttl=
22	19.173327	10.71.1.68	1.2.3.4	ICMP	74	Echo (ping) request id=0x0001, seq=77/19712, ttl=
23	24.144428	10.71.1.68	1.2.3.4	ICMP	74	Echo (ping) request id=0x0001, seq=78/19968, ttl=
24	29.143262	10.71.1.68	1.2.3.4	ICMP	74	Echo (ping) request id=0x0001, seq=79/20224, ttl=
25	34.141938	10.71.1.68	1.2.3.4	ICMP	74	Echo (ping) request id=0x0001, seq=80/20480, ttl=
26	39.140222	10.71.1.68	1.2.3.4	ICMP	74	Echo (ping) request id=0x0001, seq=81/20736, ttl=

```

> Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_2e:c6:1e (c0:25:e9:2e:c6:1e), Dst: Routerbo_31:f6:e8 (e4:8d:8c:31:f6:e8)
> Internet Protocol Version 4, Src: 10.71.1.68, Dst: 172.217.24.206
  Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d10 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 75 (0x004b)
    Sequence number (LE): 19200 (0x4b00)
    [Response frame: 10]
  Data (32 bytes)
    Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
    [Length: 32]

```

- Mở rộng phần tiêu đề của gói tin Echo (ping) reply của gói trên ta thấy trường Type là 0 cho thấy gói tin này là ICMP Echo Reply. Hơn nữa, ta có thể thấy nội dung phần Data (32 bytes) giống với gói tin ICMP Echo Request ở trên.

No.	Time	Source	Destination	Protocol	Length	Info
7	2.040262	10.71.1.68	172.217.24.206	ICMP	74	Echo (ping) request id=0x0001, seq=74/18944, ttl=
8	2.067931	172.217.24.206	10.71.1.68	ICMP	74	Echo (ping) reply id=0x0001, seq=74/18944, ttl=
→	9 3.055779	10.71.1.68	172.217.24.206	ICMP	74	Echo (ping) request id=0x0001, seq=75/19200, ttl=
←	10 3.082392	172.217.24.206	10.71.1.68	ICMP	74	Echo (ping) reply id=0x0001, seq=75/19200, ttl=
11	4.070882	10.71.1.68	172.217.24.206	ICMP	74	Echo (ping) request id=0x0001, seq=76/19456, ttl=
12	4.121663	172.217.24.206	10.71.1.68	ICMP	74	Echo (ping) reply id=0x0001, seq=76/19456, ttl=
22	19.173327	10.71.1.68	1.2.3.4	ICMP	74	Echo (ping) request id=0x0001, seq=77/19712, ttl=
23	24.144428	10.71.1.68	1.2.3.4	ICMP	74	Echo (ping) request id=0x0001, seq=78/19968, ttl=
24	29.143262	10.71.1.68	1.2.3.4	ICMP	74	Echo (ping) request id=0x0001, seq=79/20224, ttl=

< >

```
> Frame 10: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Routerbo_31:f6:e8 (e4:8d:8c:31:f6:e8), Dst: Tp-LinkT_2e:c6:1e (c0:25:e9:2e:c6:1e)
> Internet Protocol Version 4, Src: 172.217.24.206, Dst: 10.71.1.68
└ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
        Code: 0
        Checksum: 0x5510 [correct]
            [Checksum Status: Good]
        Identifier (BE): 1 (0x0001)
        Identifier (LE): 256 (0x0100)
        Sequence number (BE): 75 (0x004b)
        Sequence number (LE): 19200 (0x4b00)
            [Request frame: 9]
            [Response time: 26.613 ms]
    Data (32 bytes)
        Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
            [Length: 32]
```

### 11.2.2. Sử dụng công cụ tracert

- Bước 1:** Mở Windows Explorer vào đường dẫn cài đặt, khởi động Wireshark (ví dụ đường dẫn mặc định là: C:\Program Files\Wireshark\Wireshark.exe).
- Bước 2:** Mở Command Prompt thực hiện lệnh tracert như dưới đây:

```
C:\Users\ttmlab>tracert google.com

Tracing route to google.com [172.217.24.206]
over a maximum of 30 hops:

 1  20 ms   101 ms   41 ms  bknet71.hust.edu.vn [10.71.0.1]
 2  112 ms   37 ms   30 ms  202.191.59.17
 3  113 ms   39 ms   23 ms  202.191.57.1
 4   8 ms    8 ms   65 ms  118.71.255.33
 5   62 ms   37 ms  204 ms  10.245.32.228
 6   56 ms   59 ms   92 ms  113.22.5.118
 7  130 ms   39 ms   33 ms  118.69.253.73
 8   36 ms   27 ms   39 ms  74.125.49.162
 9   *       *       * Request timed out.
10   24 ms   27 ms   48 ms  172.253.69.224
11   25 ms   44 ms   32 ms  108.170.241.48
12   53 ms   24 ms   24 ms  216.239.62.165
13   25 ms   32 ms   24 ms  209.85.250.118
14   26 ms   29 ms   65 ms  108.170.241.97
15   33 ms   33 ms   24 ms  209.85.143.123
16   31 ms   26 ms   48 ms  hkg12s13-in-f14.1.e100.net [172.217.24.206]

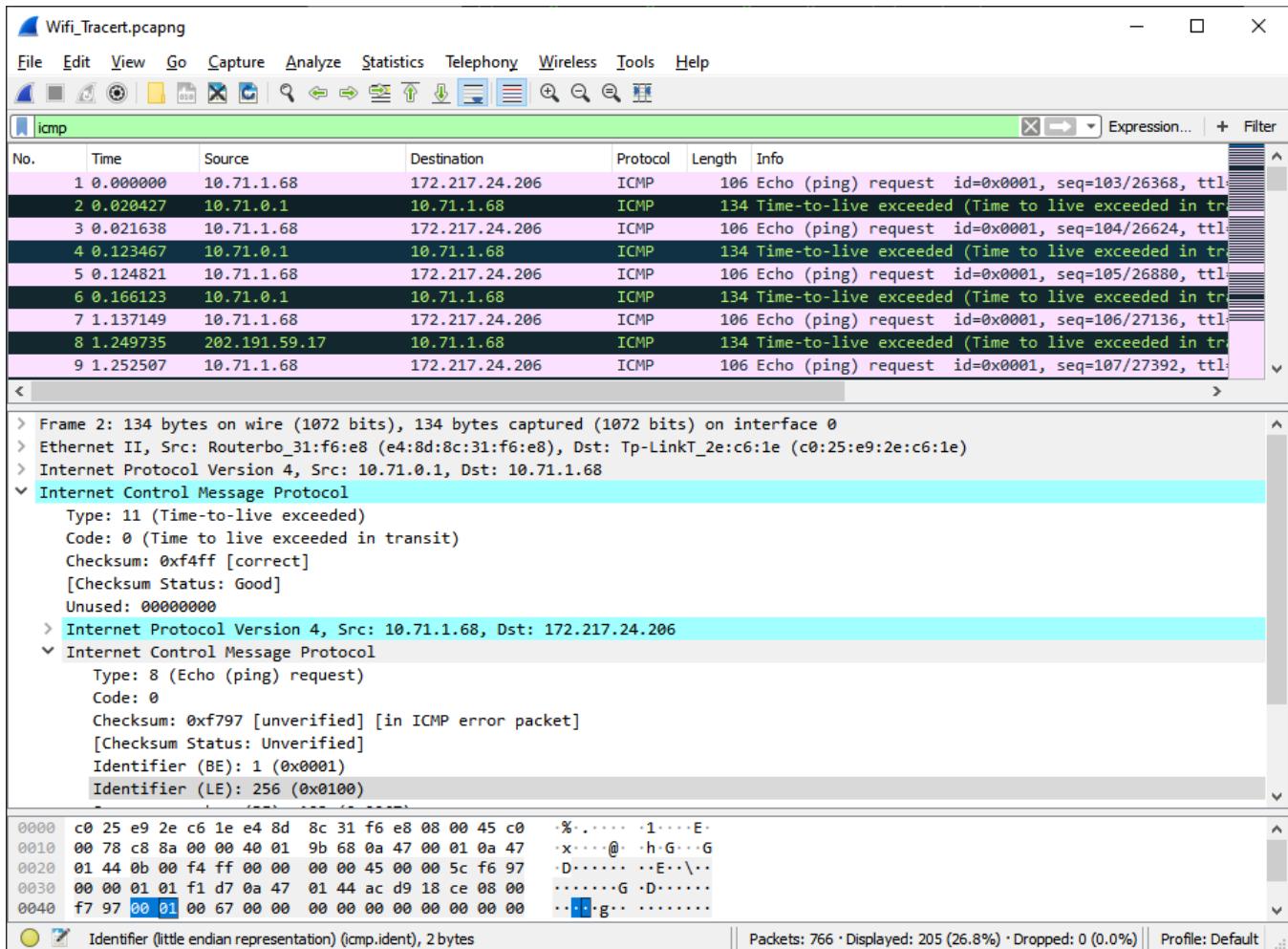
Trace complete.
```

- Bước 3:** Sau khi lệnh tracert ở trên kết thúc, thực hiện lệnh tracert lần 2 như sau:

```
C:\Users\ttmlab>tracert 1.2.3.4

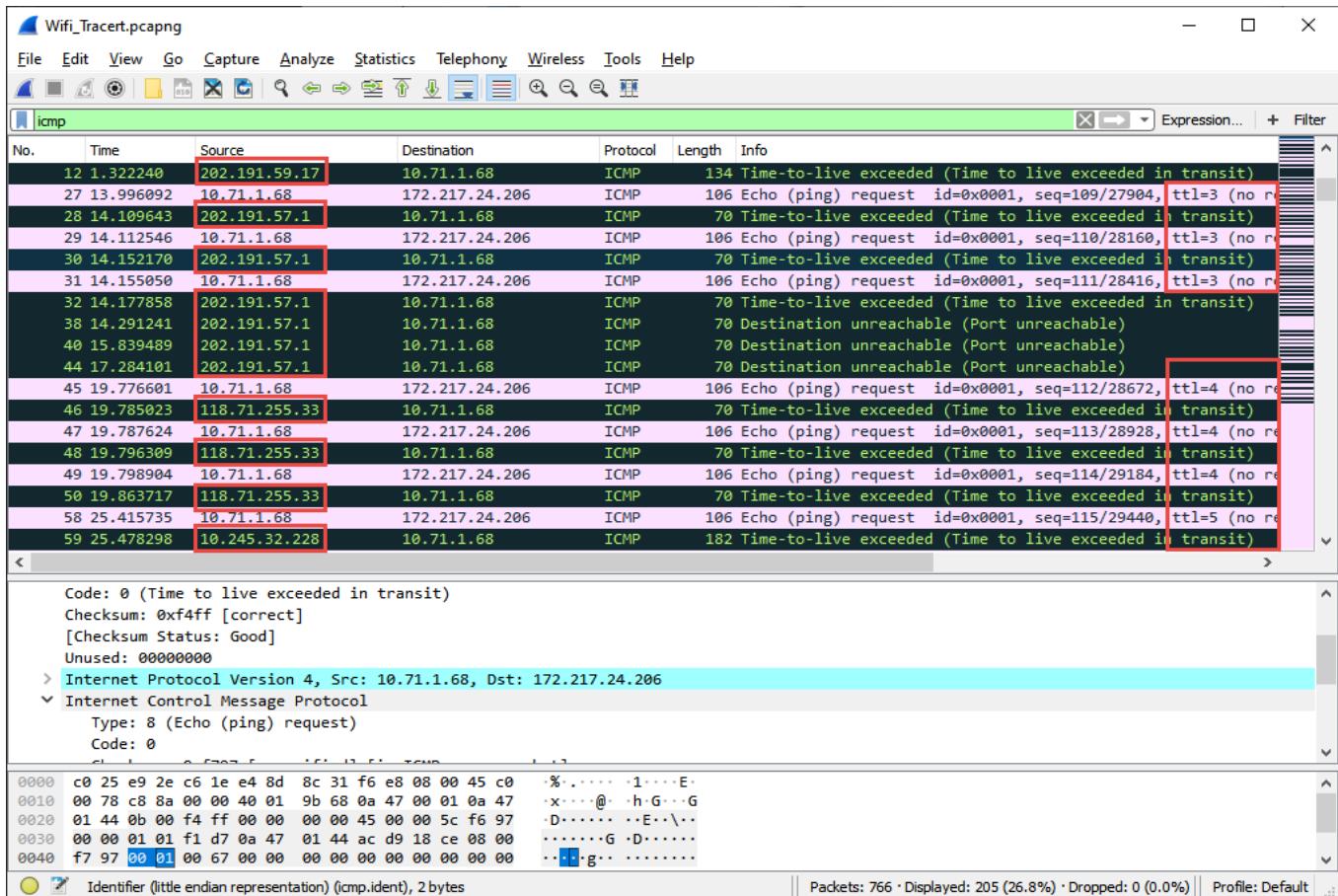
Tracing route to 1.2.3.4 over a maximum of 30 hops
  1  35 ms    5 ms    5 ms  bknet71.hust.edu.vn [10.71.0.1]
  2  43 ms    3 ms   22 ms  202.191.59.17
  3  5 ms     3 ms    7 ms  202.191.57.1
  4  6 ms    31 ms    4 ms  118.71.255.33
  5  *        13 ms    *   10.245.32.228
  6  38 ms    34 ms   26 ms  42.114.255.93
  7  *        *       *   Request timed out.
  8  *        *       *   Request timed out.
  9  *        *       *   Request timed out.
 10  *        *       *   Request timed out.
 11  *        *       *   Request timed out.
 12  *        *       *   Request timed out.
 13  *        *       *   Request timed out.
 14  *        *       *   Request timed out.
 15  *        *       *   Request timed out.
 16  *        *       *   Request timed out.
```

- **Bước 4:** Ngừng bắt gói tin trên Wireshark.
- **Bước 5:** Trên Wireshark điền xâu icmp vào bộ lọc để lọc lấy các gói tin ICMP. Kết quả nhận được sẽ tương tự như sau:



### Phân tích kết quả:

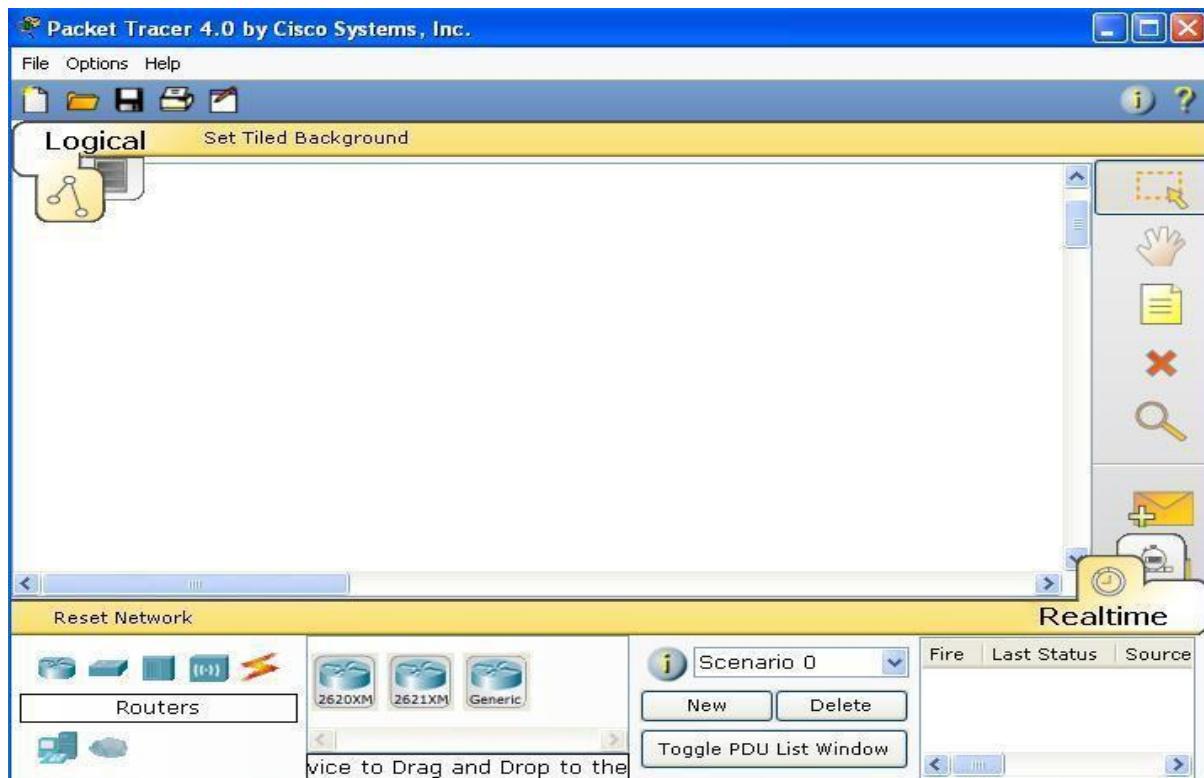
- Kết quả của lệnh tracert ở bước 2 cho thấy từ máy tính thực hiện tới máy chủ google.com có **16** chặng đi qua với địa chỉ IP của mỗi chặng đã được liệt kê.
- Kết quả của lệnh tracert ở bước 3 cho thấy bắt đầu từ chặng thứ **7**, lệnh này không phân tích được địa chỉ. Như vậy, có thể phán đoán, kết nối của máy tính thực hiện lệnh tới máy 1.2.3.4 bắt đầu có lỗi từ bước này.
- Trên kết quả bắt gói tin của Wireshark, chúng ta có thể thấy các nhóm 3 gói tin ICMP được gửi đi. Sau khi gửi xong một nhóm, giá trị TTL của nhóm tiếp theo tăng thêm 1. Địa chỉ nguồn của các gói tin báo lỗi ICMP Time to live exceeded chính là địa chỉ các chặng.



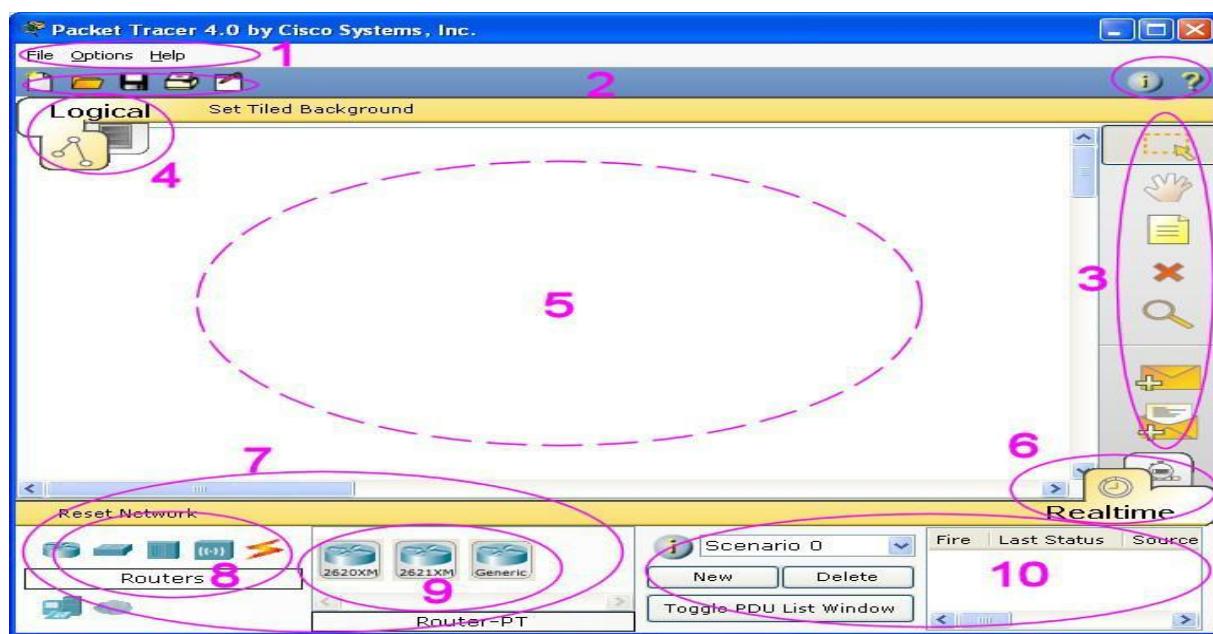
## 8. PHỤ LỤC 5: HƯỚNG DẪN SỬ DỤNG PACKET TRACER

### 12.1. Hướng dẫn sử dụng cơ bản

Giao diện chính của chương trình như sau:



Các khu vực làm việc chính của chương trình:



Chi tiết chức năng các MENU:

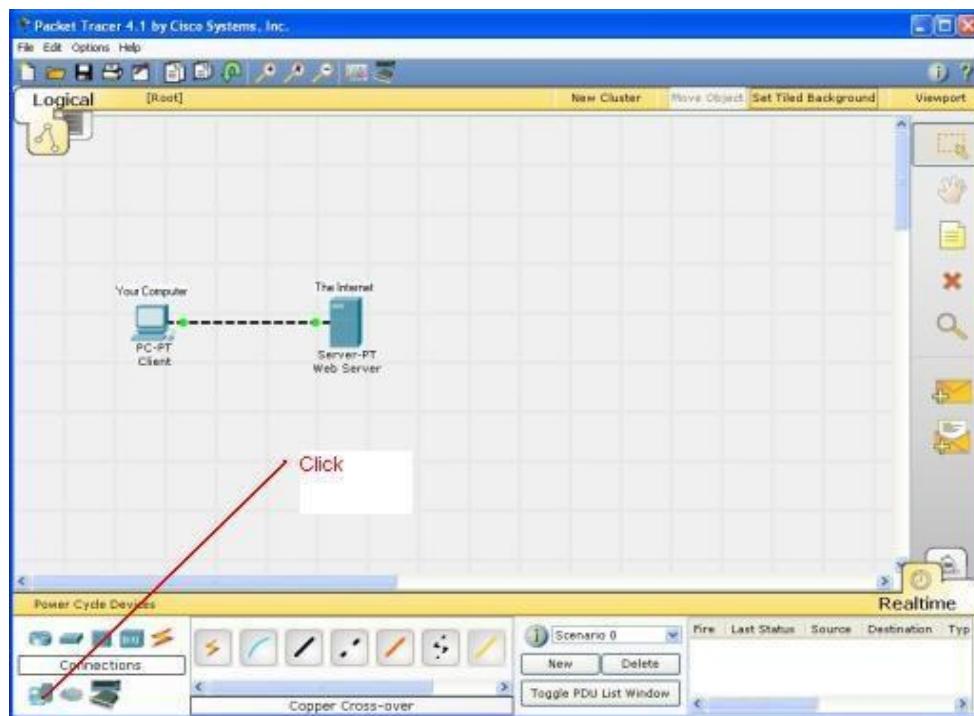
- 1. Menu Bar** : bao gồm các menu **File**, **Options**, **Edit** và **Help** cung cấp các chức năng cơ bản như **Open**, **Save**, **Print...**
- 2. Main Tool Bar** : gồm những nút chức năng cơ bản của menu File và Edit
- 3. Common Tools Bar** : Gồm các chức năng **Select**, **Move Layout**, **Place Note**, **Delete**, **Inspect**, **Add Simple PDU**, và **Add Complex PDU**
- 4. Logical/Physical Workspace and Navigation Bar** : Có thể chọn qua lại giữa Physical Workspace và the Logical Workspace
- 5. Workspace** : Đây là môi trường để bạn thực hiện thiết kế hệ thống mạng, xem giả lập các thiết bị và các thông tin liên quan...
- 6. Realtime/Simulation Bar**: bạn có thể chuyển qua lại giữa **Realtime** và **Simulation mode**
- 7. Network Component Box** : Nơi bạn lựa chọn các thiết bị và kết nối giữa chúng...
- 8. Device-Type Selection Box** : Gồm những thiết bị được Packet Tracer 4.1 hỗ trợ

9. **Device-Specific Selection Box** : lựa chọn những thiết bị dùng trong hệ thống mạng và cách thức nối kết giữa chúng

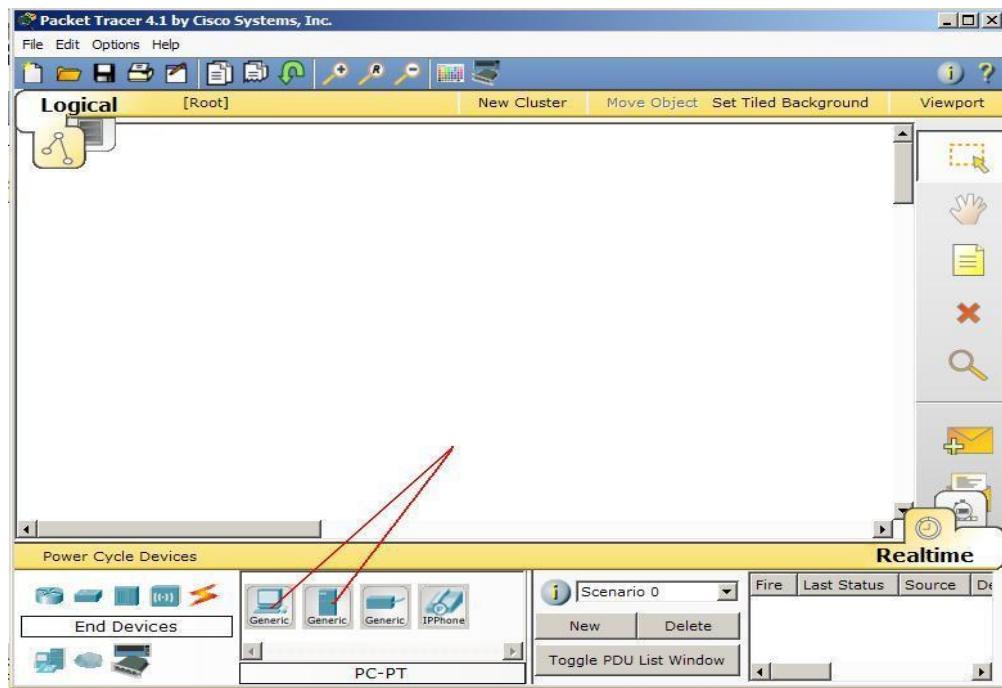
10. **User Created Packet Window\*** : Quản lí các packets mà bạn đặt trong hệ thống mạng. Xem "Simulation Mode" để nắm rõ hơn về chức năng này

## 12.2. Hướng dẫn tạo hệ thống đơn giản bao gồm 1 PC và 1 Server kết nối với nhau

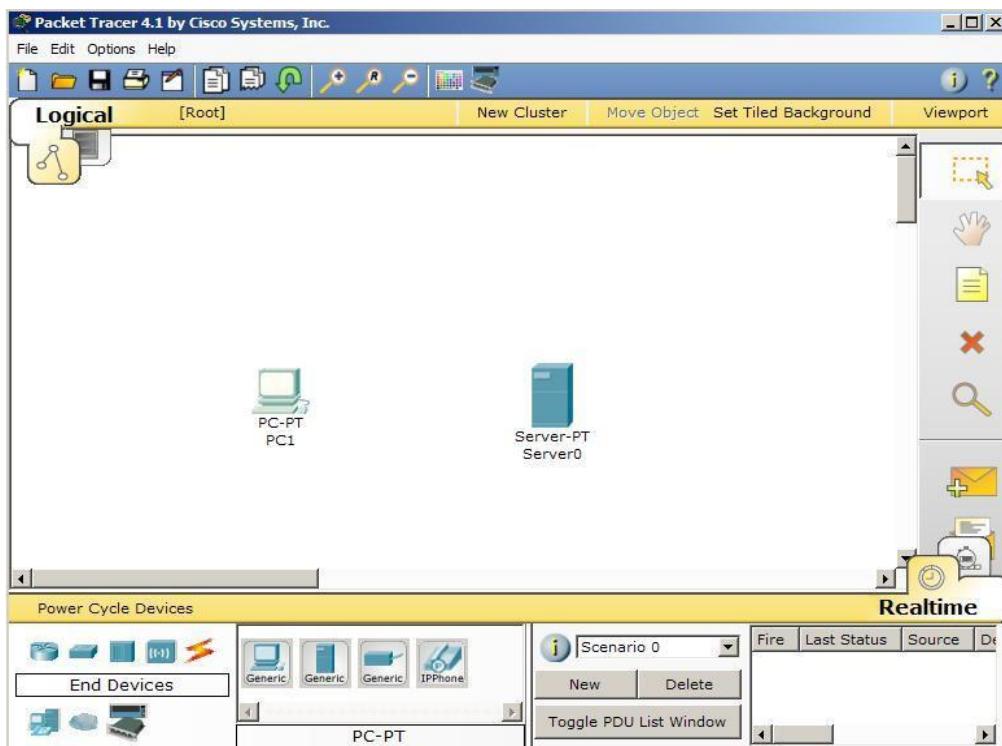
Trong chế độ làm việc **LOGICAL**, bạn lưu ý khu vực số 7, bạn chọn biểu tượng có hình chiếc máy vi tính . Click vào đó:



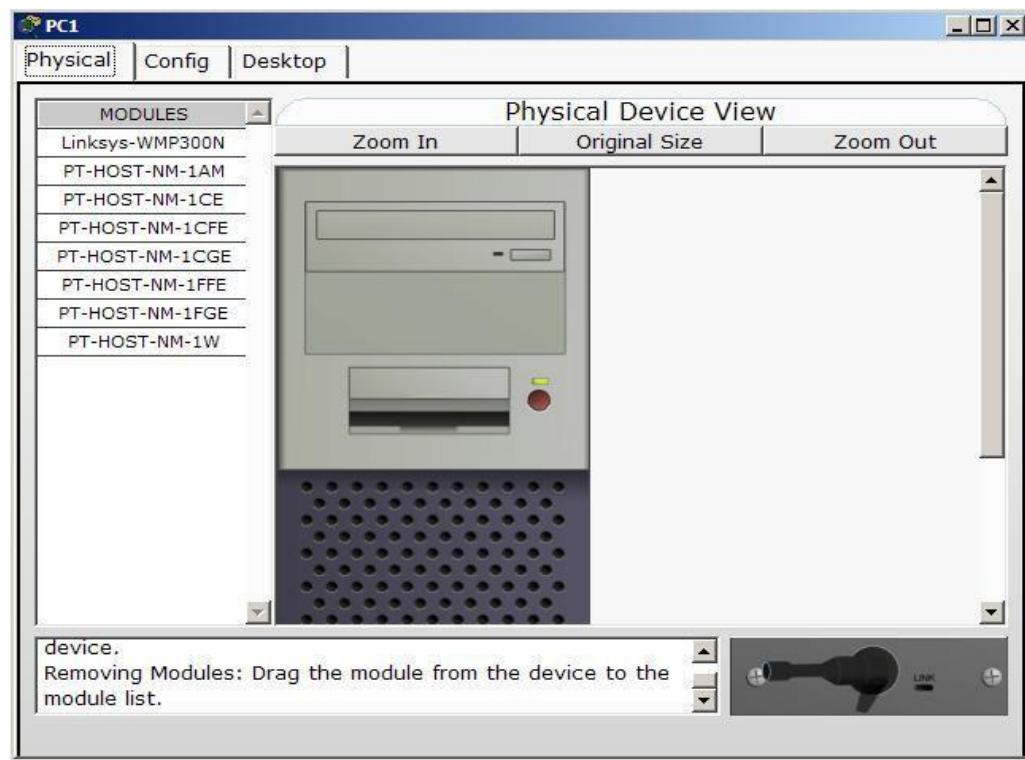
Lần lượt lựa chọn 2 thiết bị cần kết nối là **PC** và **Server**



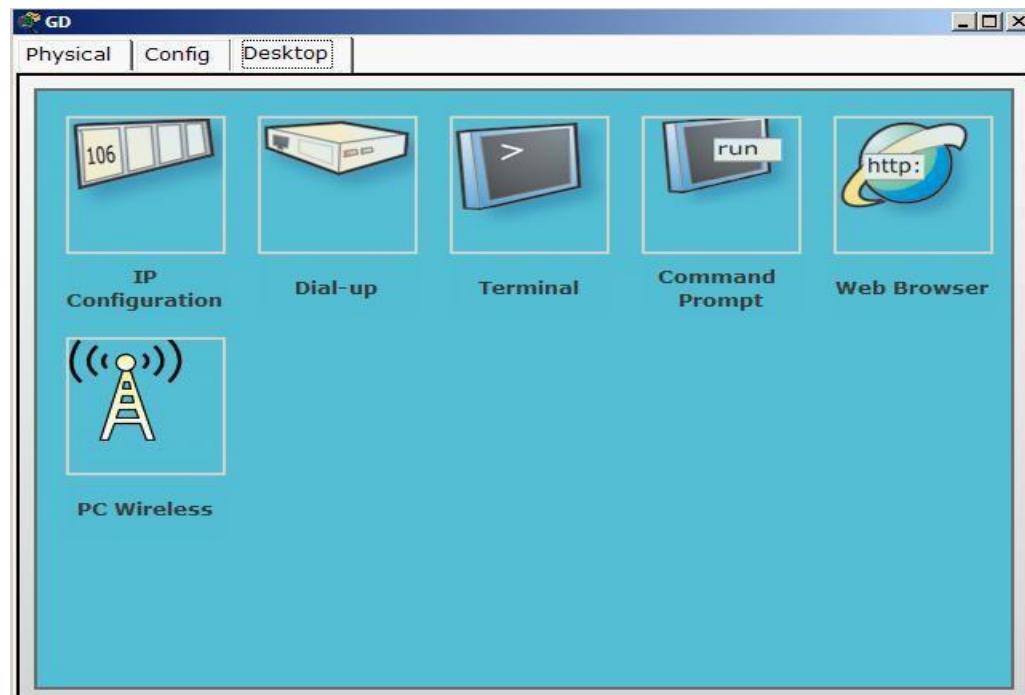
Sau đó lần lượt kéo chúng ra màn hình làm việc như sau:



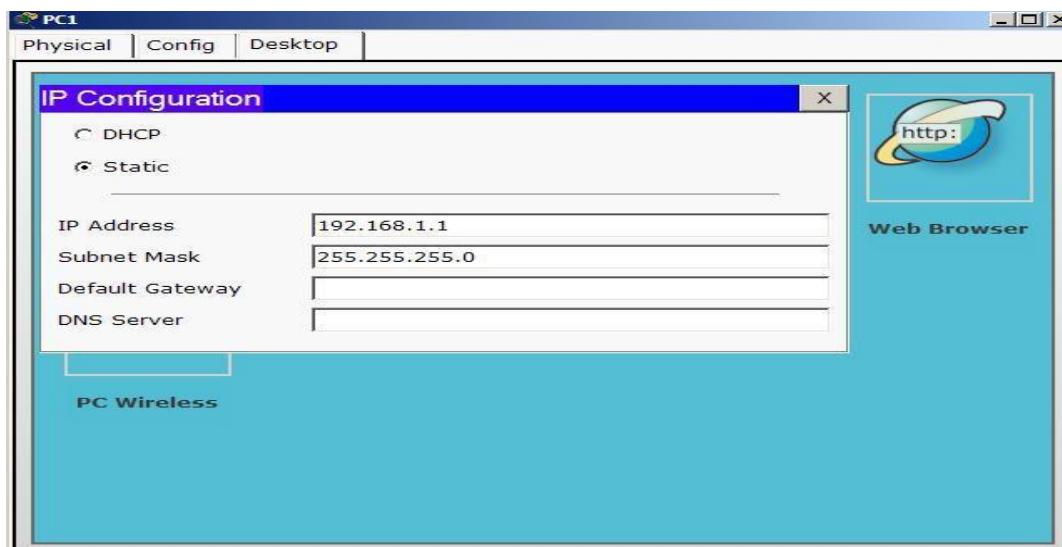
**Click** vào biểu tượng PC trên, chúng ta có thể có thêm những thông tin chi tiết về nó, và có thể tiến hành cài đặt các thông số cho PC đó trên mạng như IP, Gateway, tên máy, loại thiết bị dùng để kết nối vào mạng...



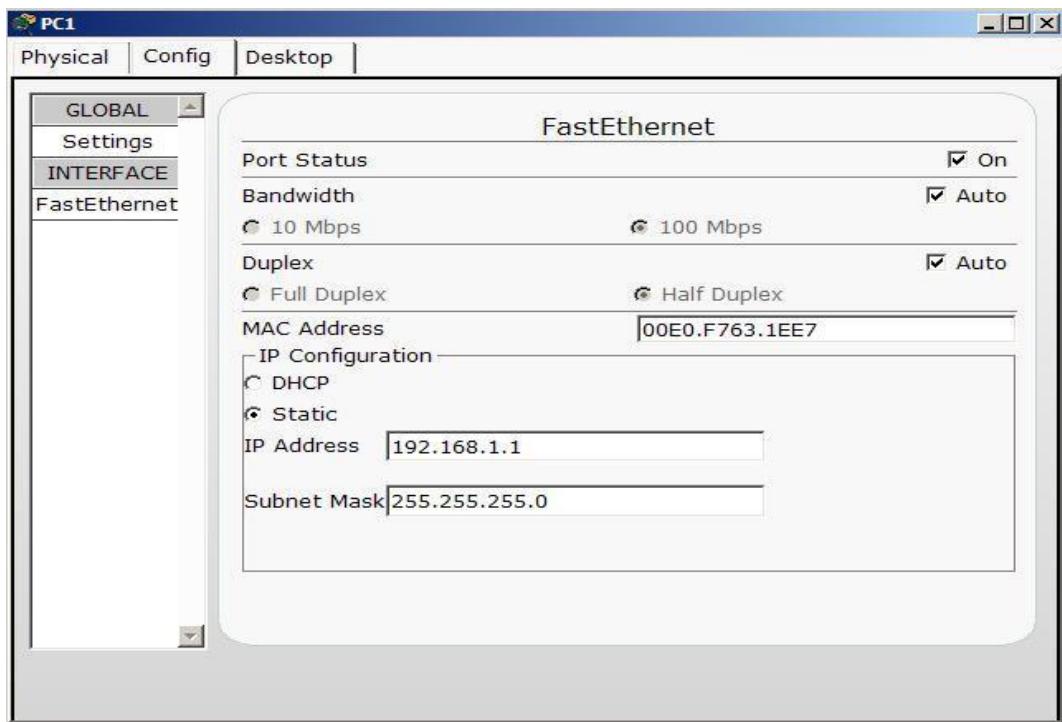
Để cấu hình IP của máy, ta chọn Tab **DESKTOP**:



Sau đó chọn **IP Configuration** để tiến hành cấu hình IP cho máy:

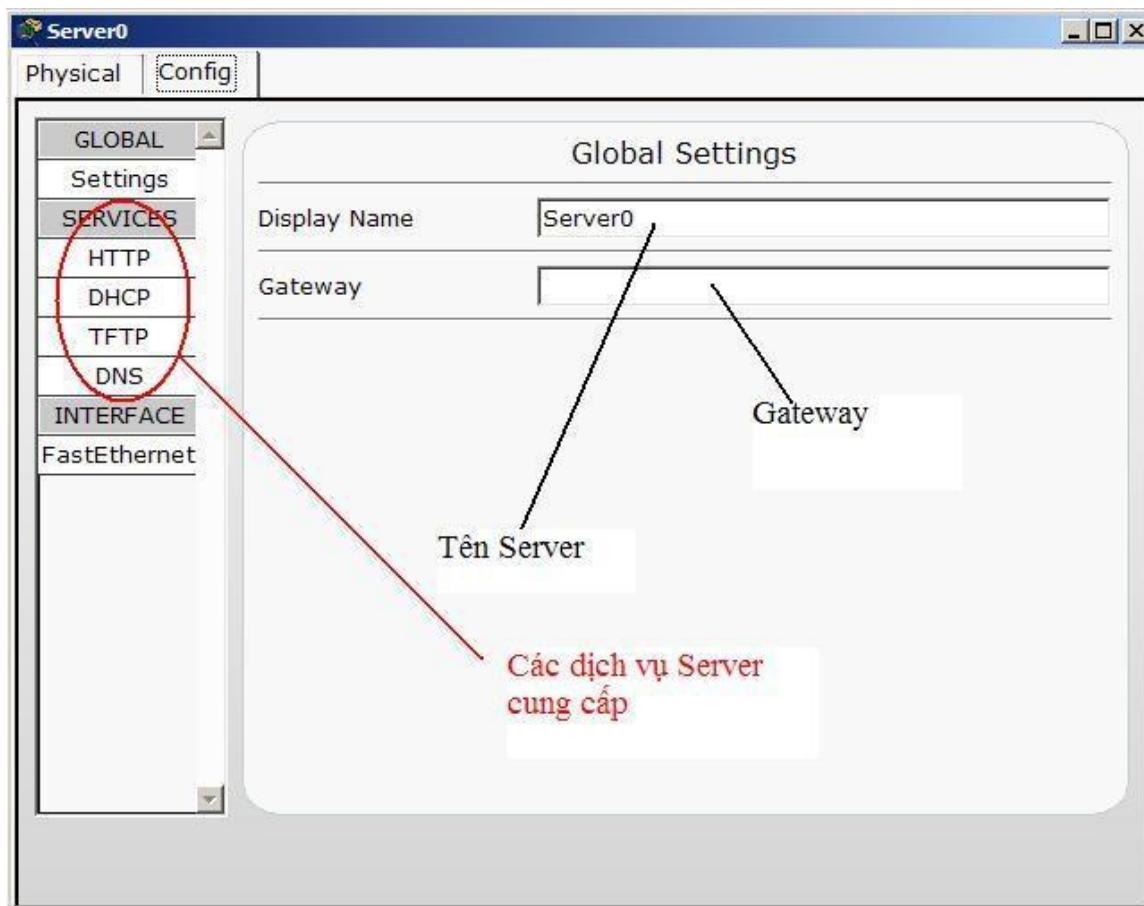


Nếu muốn thay đổi tên máy thì chúng ta chọn **Tab CONFIG**, trong đó sẽ có những lựa chọn cho phép chúng ta xem các thông tin hiện tại của máy tính như: tên máy, địa chỉ Mac, Ip và Gateway hiện thời...

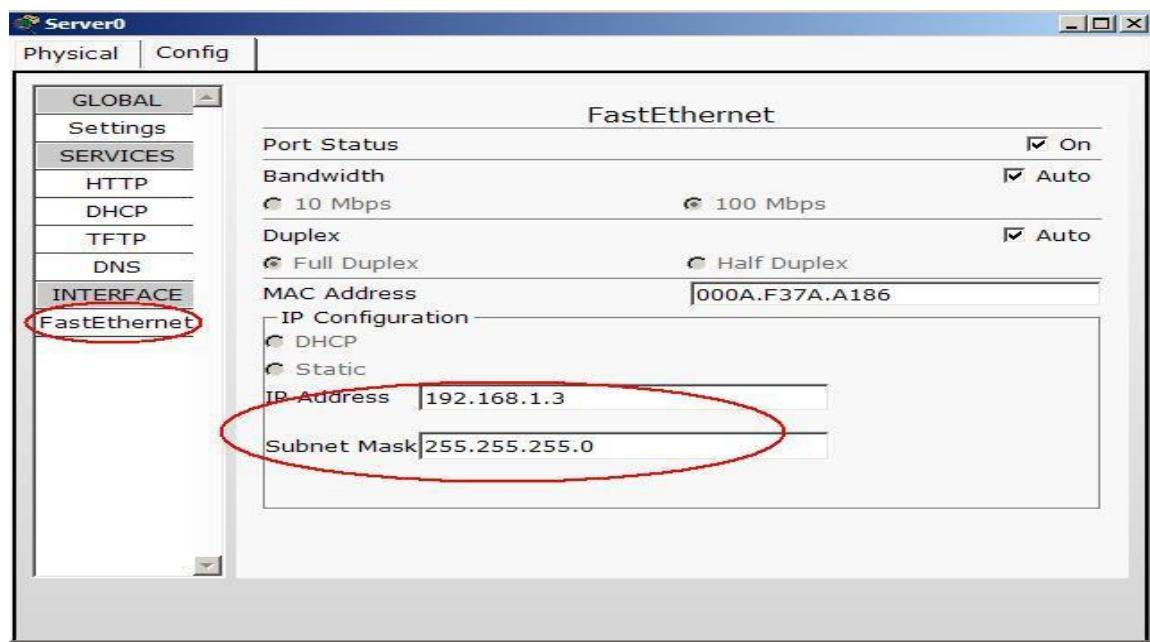


Để tiến hành **cấu hình Server**, chúng ta cũng làm tương tự, click vào hình Server , 1 bảng các thông tin chi tiết sẽ giúp chúng ta biết và tiến hành cài đặt các thông số cho Server như IP, các dịch vụ HTTP, DNS...

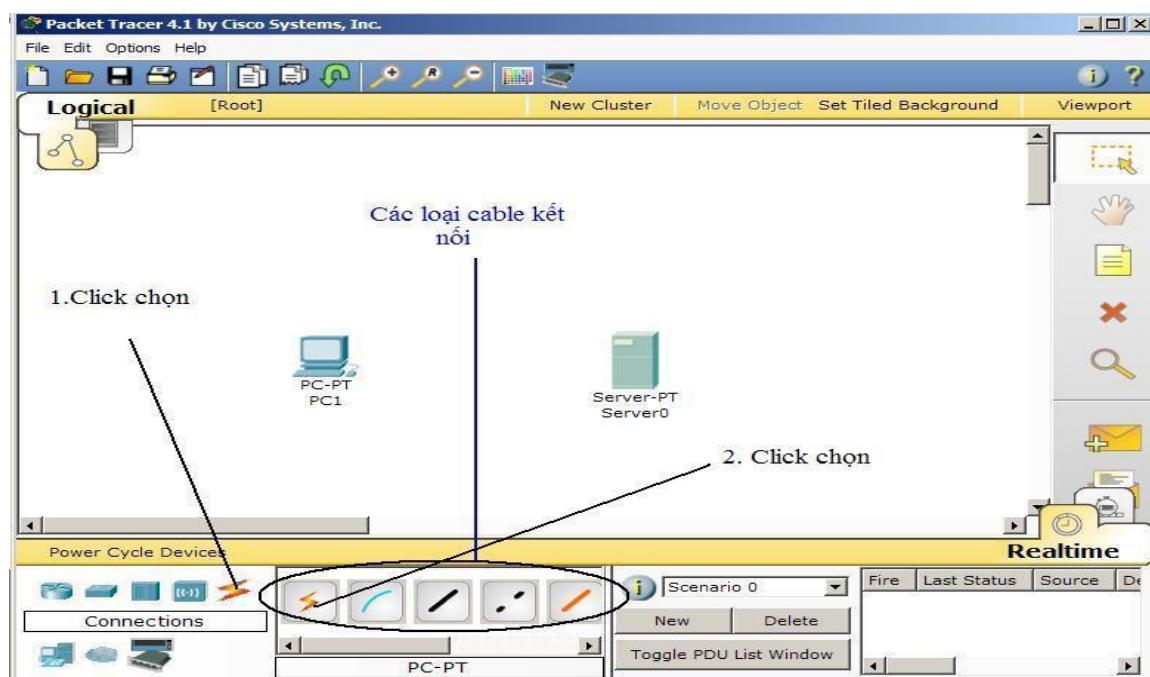
Các thông số cài đặt ở Tab **CONFIG**



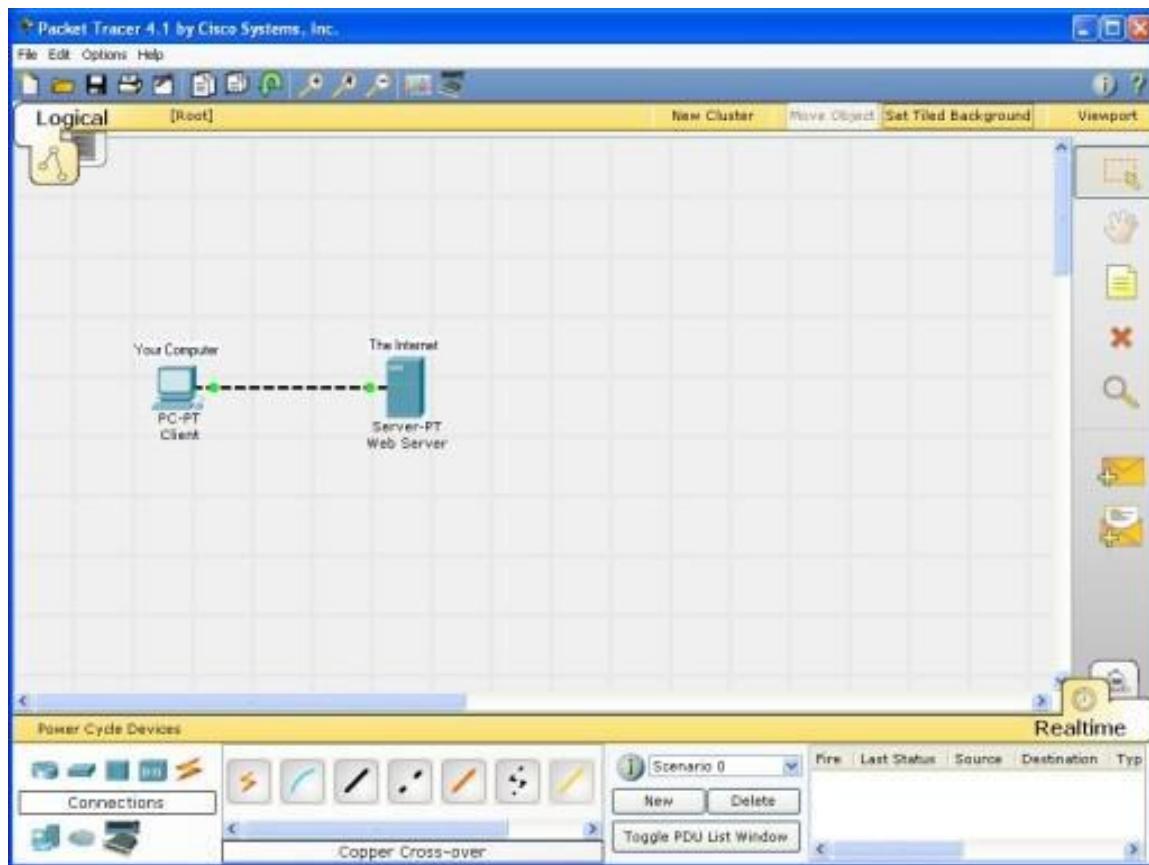
Để cấu hình địa chỉ IP cho Server chúng ta chọn FastEthernet. Sau đó tiến hành cấu hình địa chỉ IP và Subnet Mask cho Server



Bây giờ chúng ta sẽ tiến hành nối kết PC và Server lại: Bạn chọn như hướng dẫn sau



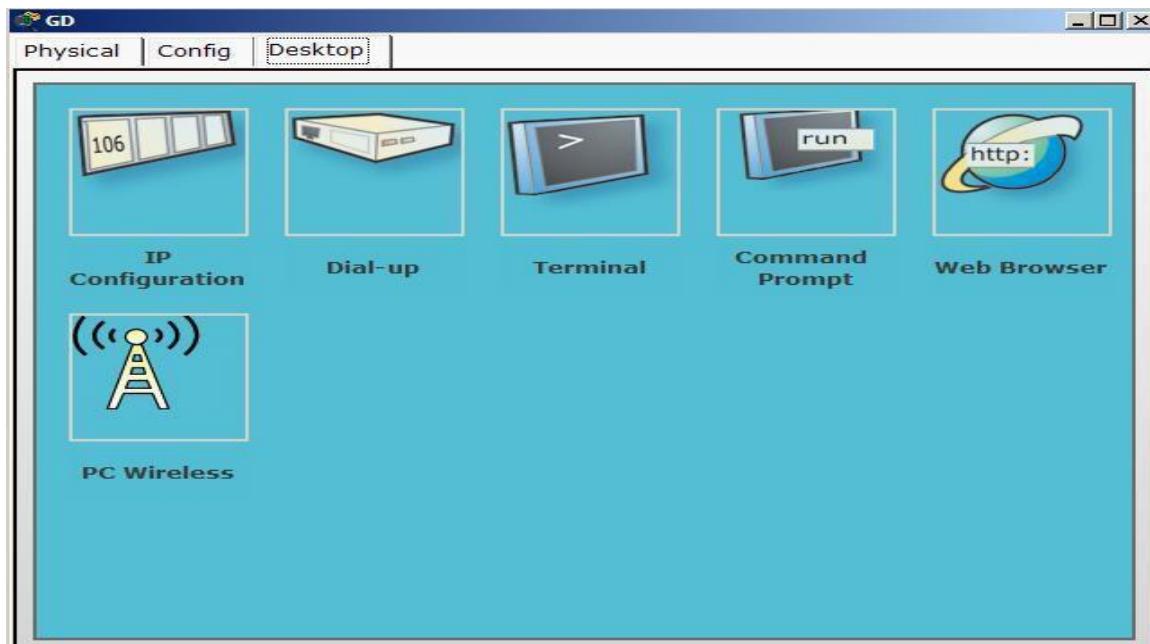
Sau đó chúng ta click vào biểu tượng PC và kết nối với Server như hình sau:



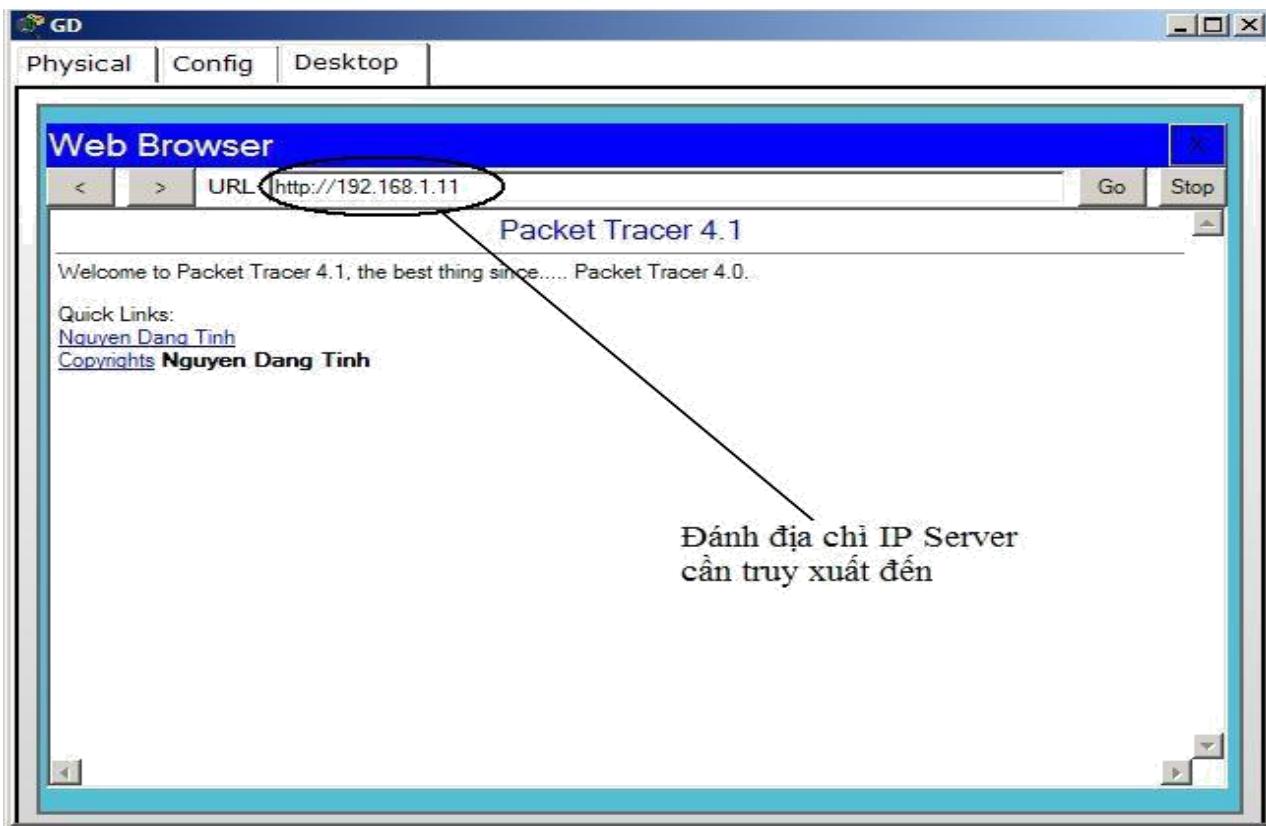
## 12.3. Hướng dẫn sử dụng được những dịch vụ mà Server cung cấp

### 12.3.1. Sử dụng dịch vụ HTTP:

Bạn Click vào biểu tượng PC, sau đó chọn tab **DESKTOP**, chúng ta sẽ có giao diện với các chức năng như sau :



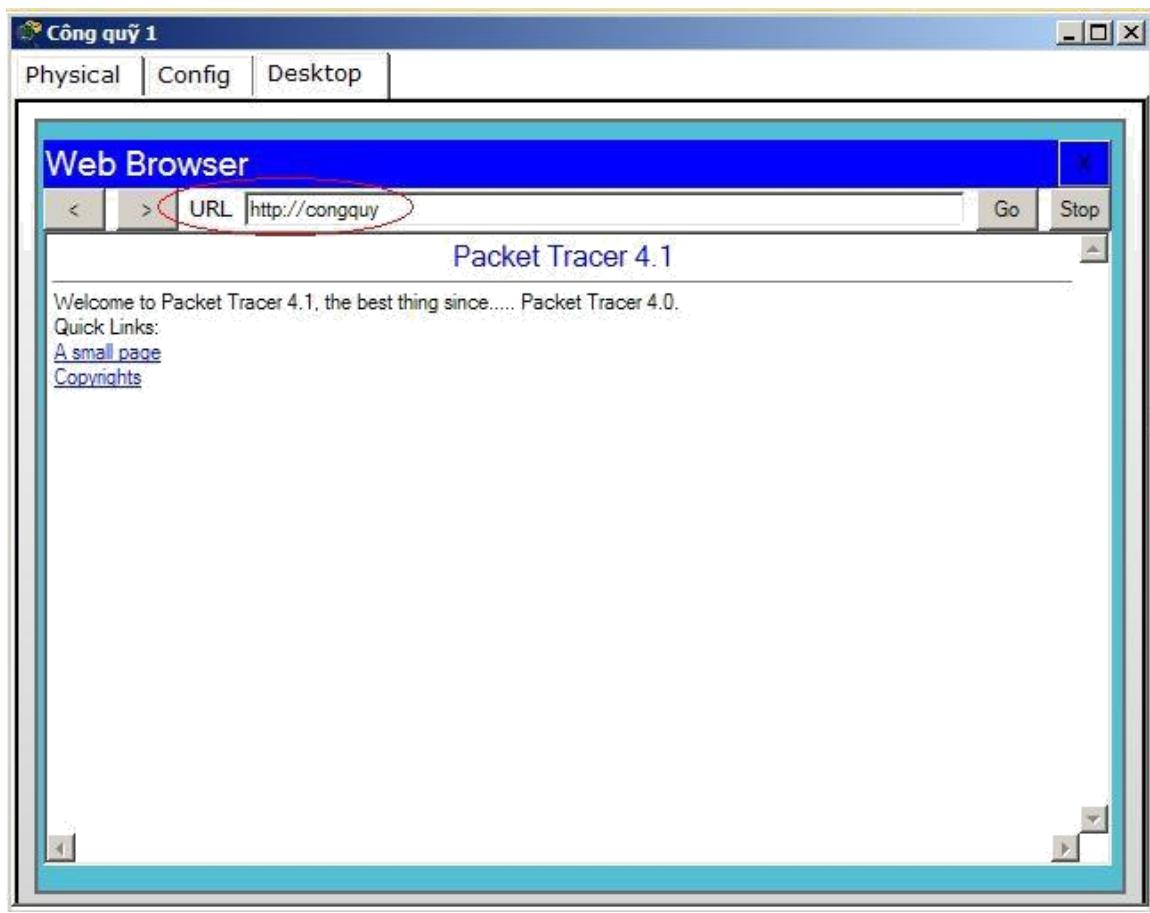
Chọn **Web Browser**, ta sẽ có 1 trình duyệt Web đơn giản giúp chúng ta có thể sử dụng dịch vụ HTTP do Server cung cấp:



Nếu truy xuất thành công đến Server, chúng ta sẽ thấy được nội dung trang INDEX như trên

Để sử dụng dịch vụ DNS do Server cung cấp, nếu đã biết tên thì chúng ta chỉ cần đánh tên vào là có thể truy xuất đến Server mà không cần đánh địa chỉ IP ( Do địa chỉ Ip khó nhớ, tên sẽ dễ nhớ hơn)

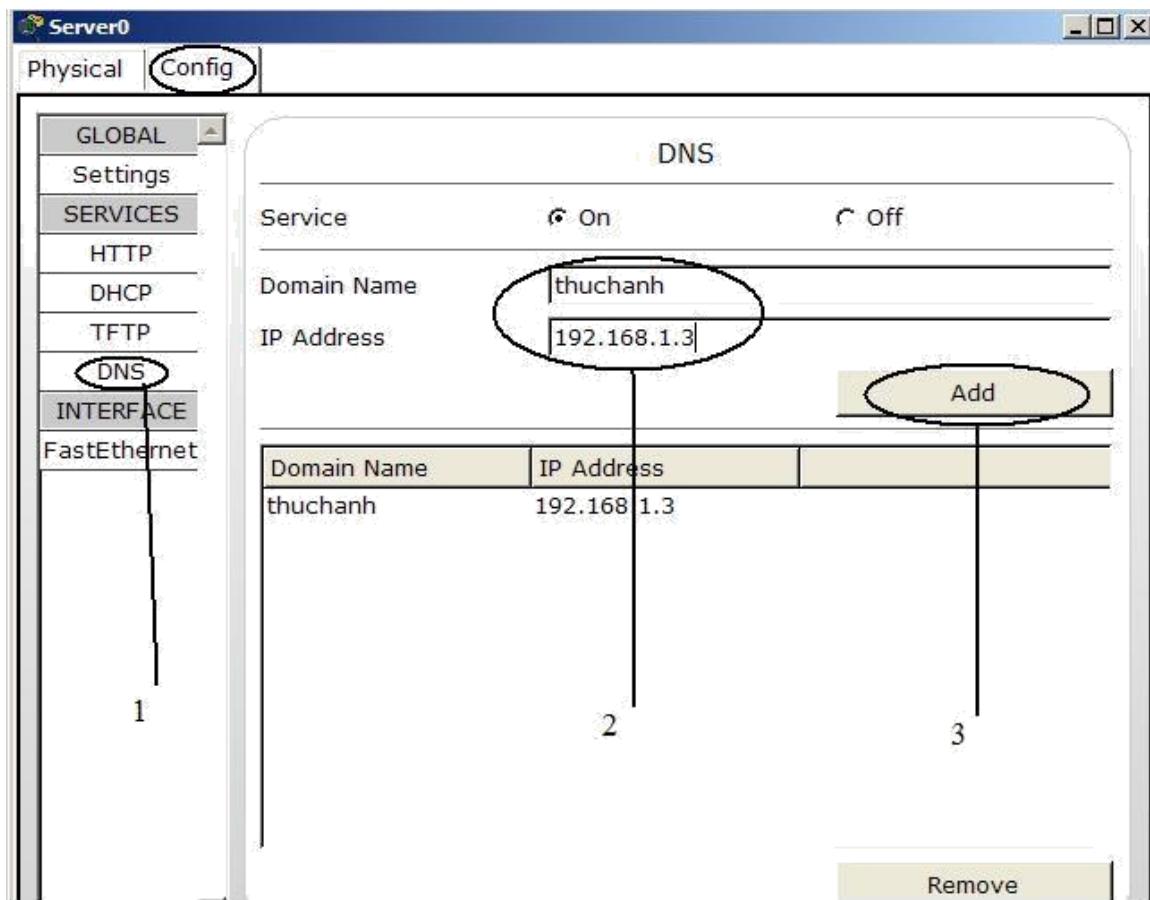
Minh họa như sau:



### 12.3.2. Hướng dẫn cài đặt dịch vụ DNS cho Server:

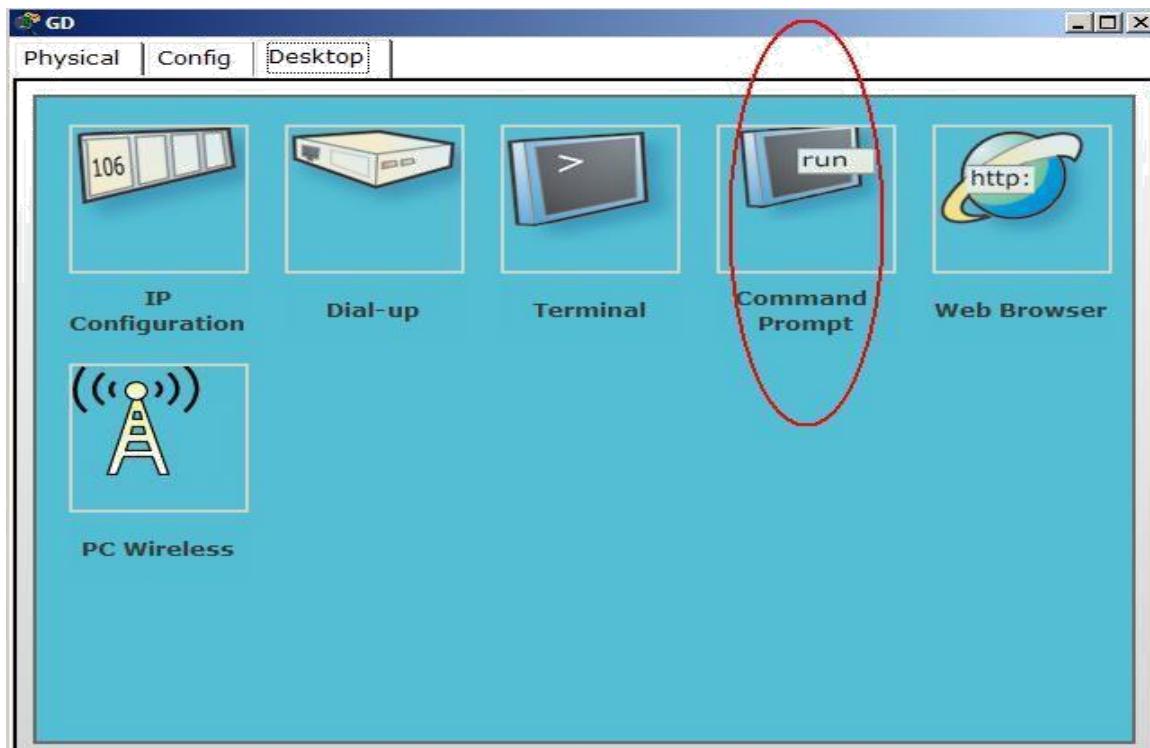
Để cài đặt dịch vụ DNS, chúng ta click đúp vào biểu tượng Server trên màn hình thiết kế.

Sau đó chọn tab **CONFIG**, chúng ta tiến hành cài đặt dịch vụ theo các bước sau :

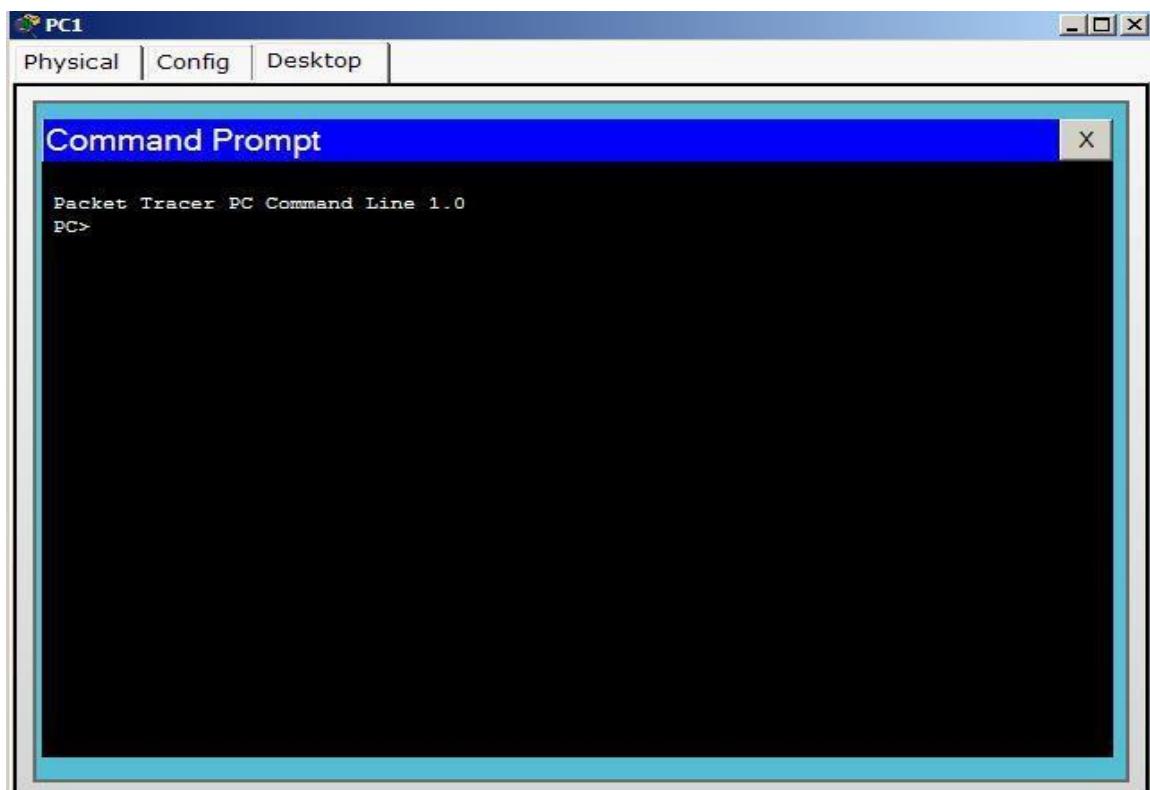


#### 12.4. Hướng dẫn thực hiện 1 số lệnh cơ bản

Để sử dụng được các lệnh này từ PC, chúng ta click chọn vào PC, sau đó chọn tab CONFIG, tiếp tục chọn **Command Prompt**

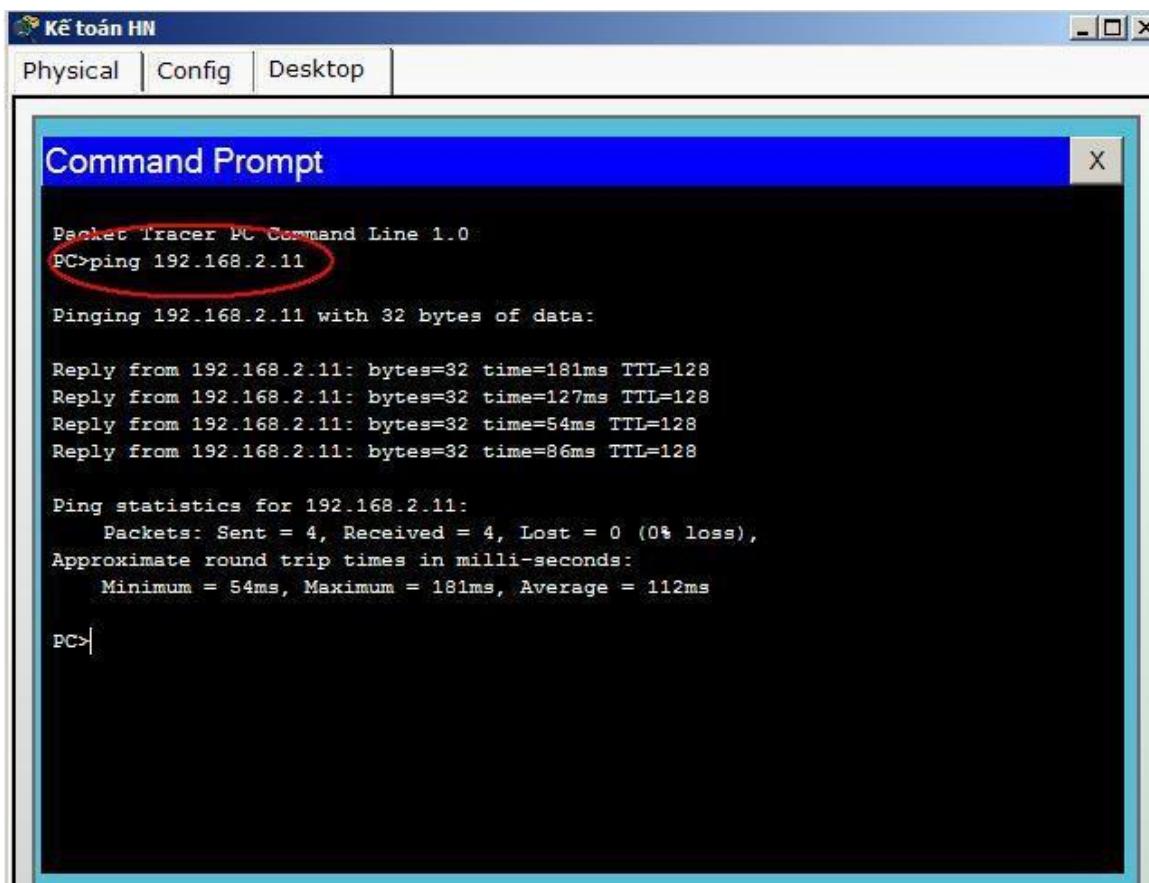


Click chọn thì giao diện hiện ra như sau:



Tại đây chúng ta có thể thực thi các câu lệnh cơ bản mà Packet Tracer hỗ trợ, sau đây là minh họa các câu lệnh cơ bản :

## 1.Lệnh PING



Kết quả lệnh Ping:

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.2.11

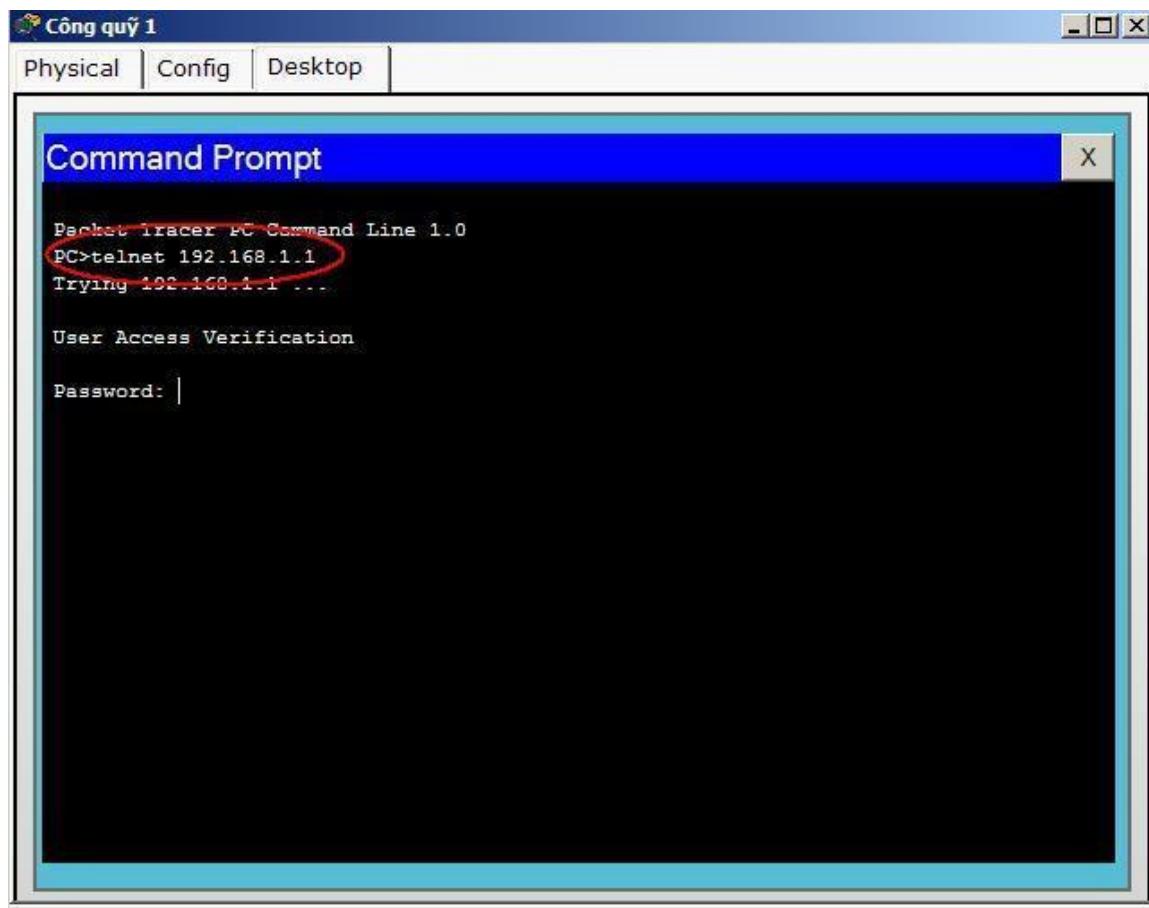
Pinging 192.168.2.11 with 32 bytes of data:

Reply from 192.168.2.11: bytes=32 time=181ms TTL=128
Reply from 192.168.2.11: bytes=32 time=127ms TTL=128
Reply from 192.168.2.11: bytes=32 time=54ms TTL=128
Reply from 192.168.2.11: bytes=32 time=86ms TTL=128

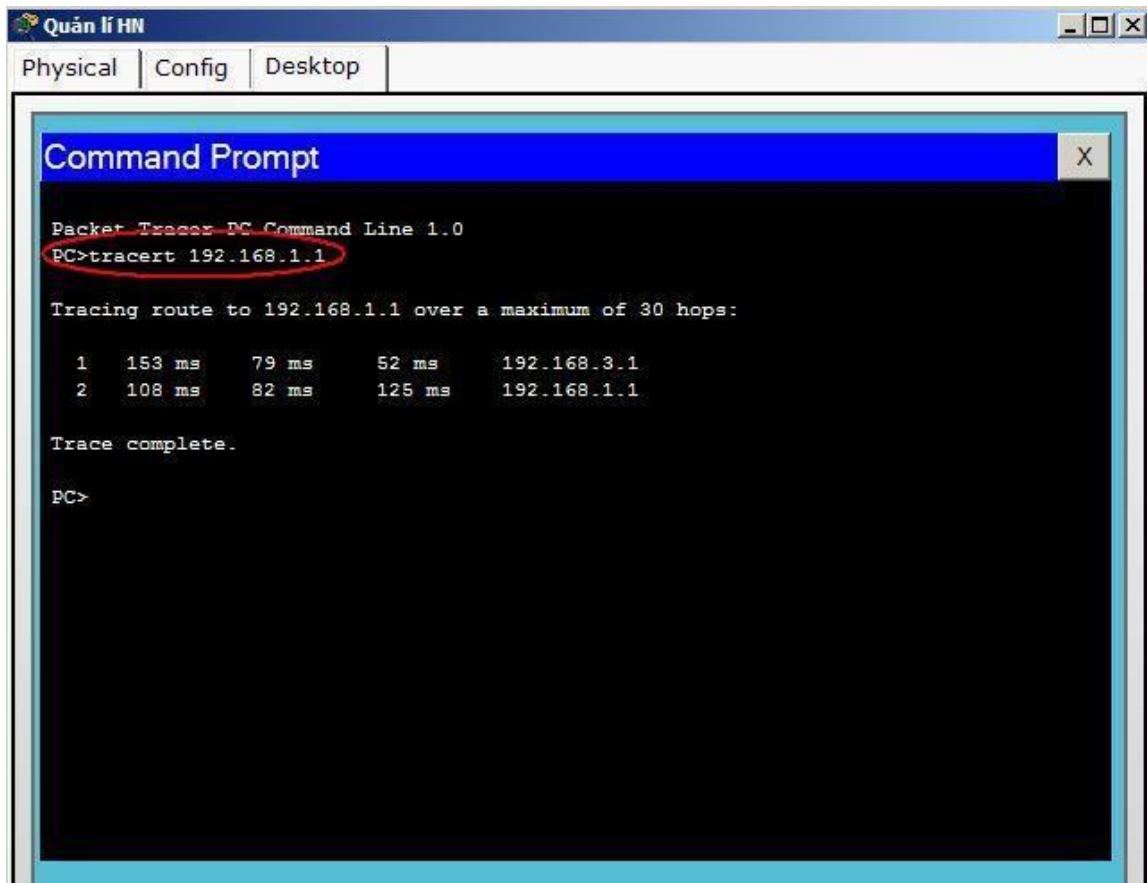
Ping statistics for 192.168.2.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 54ms, Maximum = 181ms, Average = 112ms

PC>
```

## 2.Lệnh TELNET



### 3.Lệnh TRACERT



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window is part of a larger application window titled "Quản lý HN" with tabs for "Physical", "Config", and "Desktop". The Command Prompt itself has a blue header bar with the title and a close button ("X"). The text output is as follows:

```
Packet Tracer PC Command Line 1.0
PC>tracert 192.168.1.1

Tracing route to 192.168.1.1 over a maximum of 30 hops:
  1  153 ms    79 ms      52 ms    192.168.3.1
  2  108 ms    82 ms     125 ms    192.168.1.1

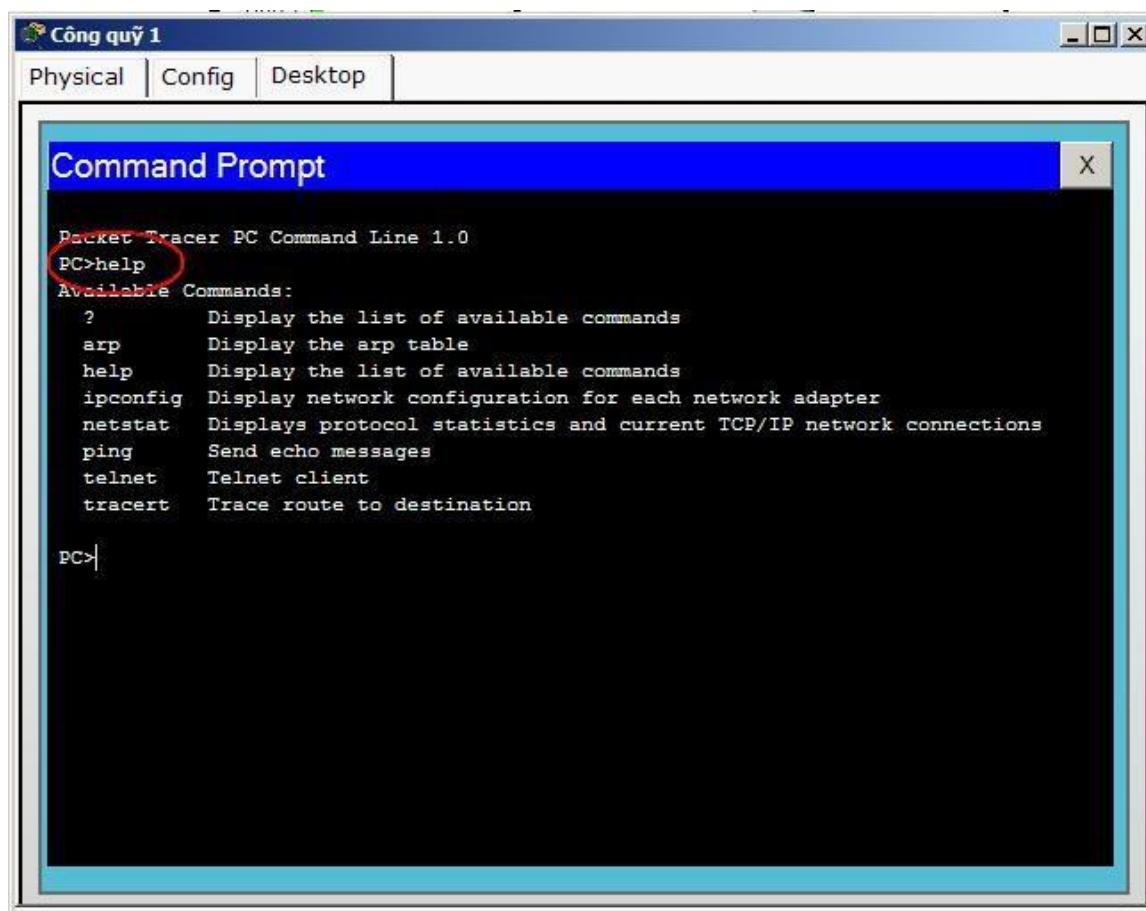
Trace complete.

PC>
```

The command "PC>tracert 192.168.1.1" is highlighted with a red oval.

Để muốn biết các thông tin chi tiết về câu lệnh chúng ta có thể đánh lệnh **HELP** hoặc ?

, Packet Tracer sẽ hiển thị thông tin các câu lệnh như sau:



The screenshot shows a Windows-style window titled "Công quỹ 1" with three tabs: "Physical", "Config", and "Desktop". The "Config" tab is selected. Inside, a command prompt window titled "Command Prompt" is displayed. The text within the window is as follows:

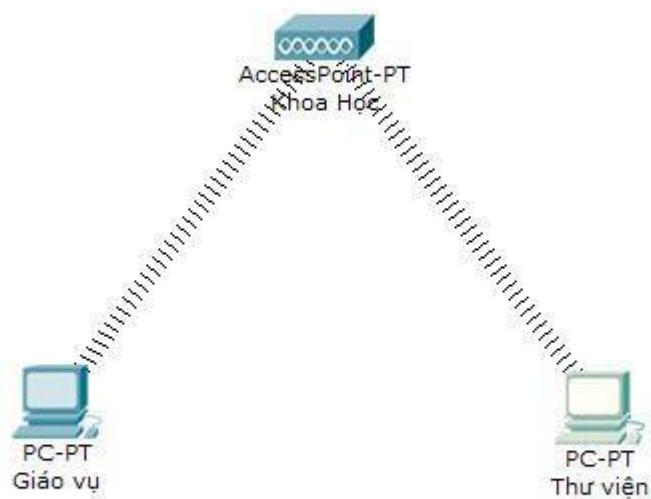
```
Packet Tracer PC Command Line 1.0
PC>help
Available Commands:
?           Display the list of available commands
arp         Display the arp table
help        Display the list of available commands
ipconfig    Display network configuration for each network adapter
netstat     Displays protocol statistics and current TCP/IP network connections
ping        Send echo messages
telnet      Telnet client
tracert    Trace route to destination

PC>
```

The word "help" is circled in red.

## 12.5. HƯỚNG DẪN THIẾT KẾ MẠNG WIRELESS ĐƠN GIẢN TRONG PACKET TRACER

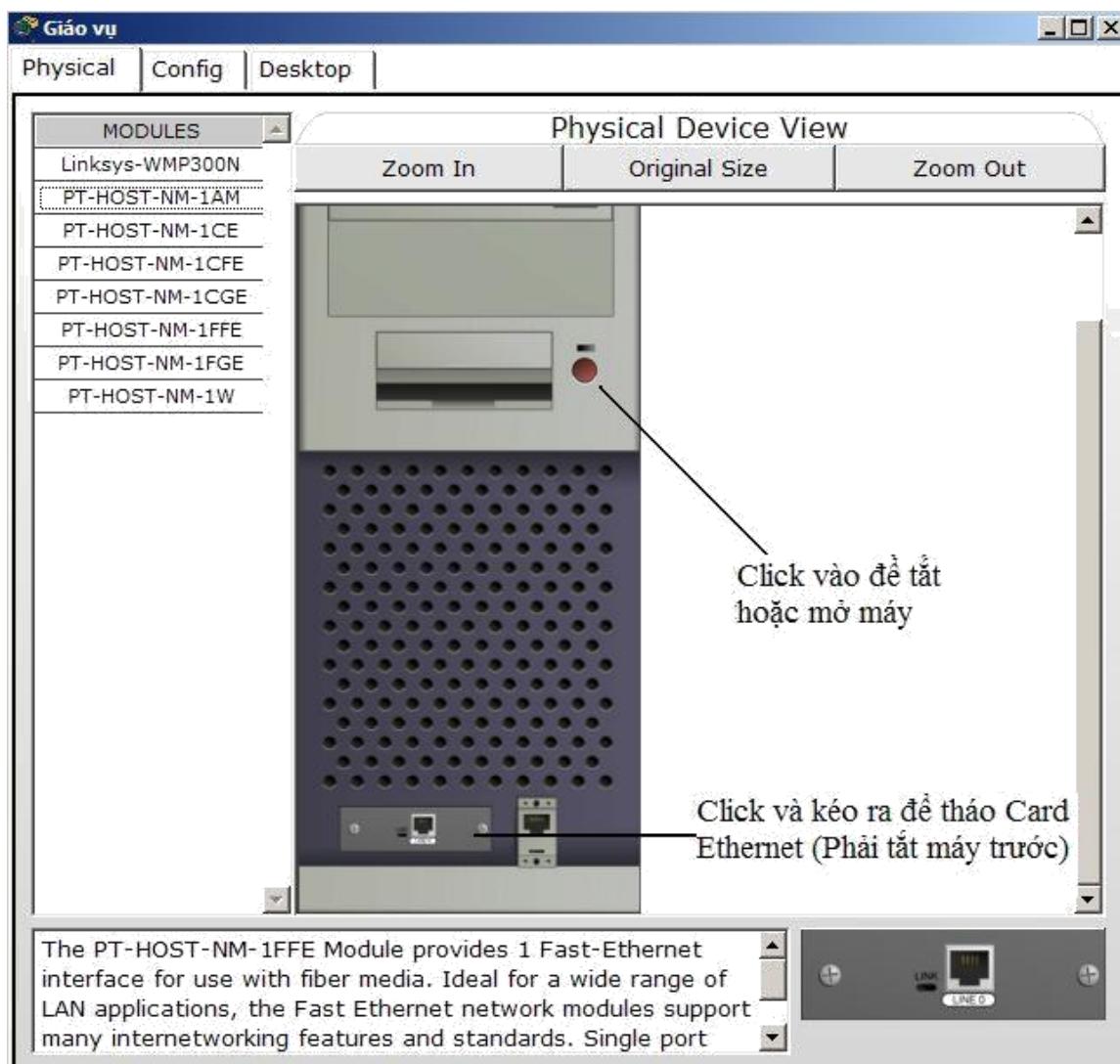
Trong phần này chúng ta sẽ tiến hành thiết kế 1 mạng Wireless đơn giản, minh họa cho mạng như hình sau :



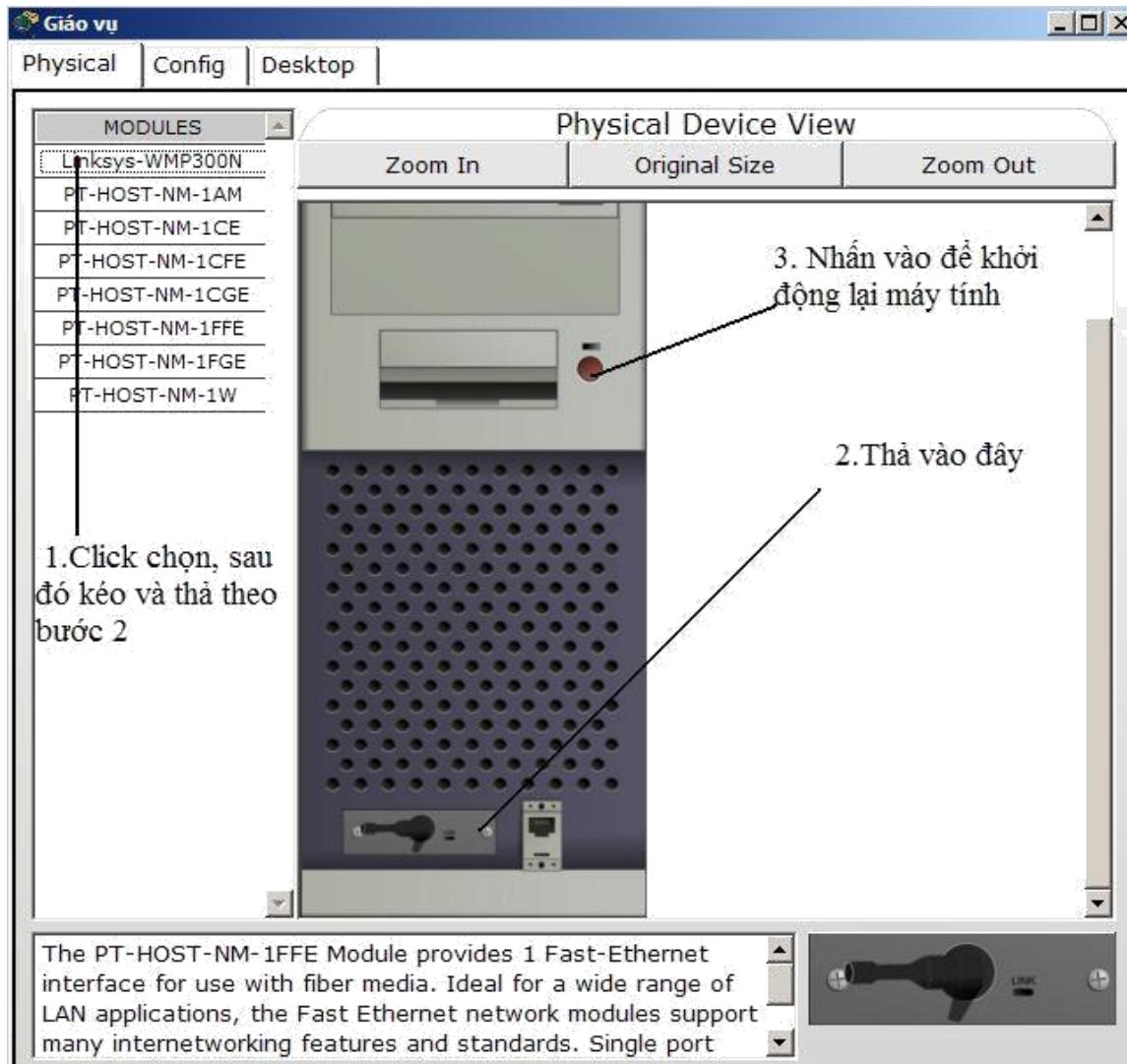
Đối với thiết kế hệ thống mạng , bố trí các thiết bị ta làm tương tự như thiết kế ở trên. Vấn đề chúng ta muốn biết ở đây là làm sao để kết nối thiết bị vào hệ thống mạng Wireless.

Chúng ta sẽ tiến hành lắp đặt Card Wireless cho hệ thống PC để có thể kết nối vào hệ thống mạng.

Đầu tiên Click vào biểu tượng PC trong thiết kế của mình, sau đó chọn **Tab Physical**, chúng ta sẽ tắt PC và tháo Card Ethenet, sau đó lắp Card Wireless cho máy. Các bước minh họa như sau:

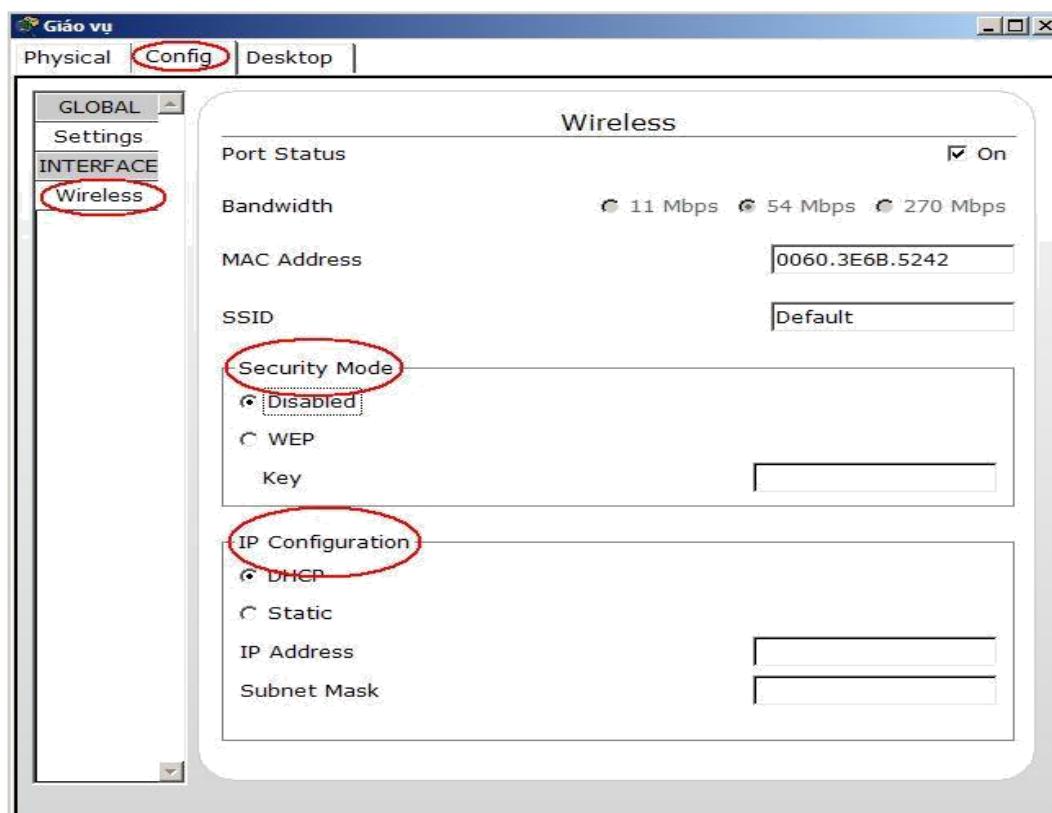


Sau khi đã tháo Card Ethernet ra, chúng ta tiến hành lắp đặt Card Wireless vào máy tính để có thể thu được sóng Wireless. Các bước tiến hành minh họa như hình dưới đây:

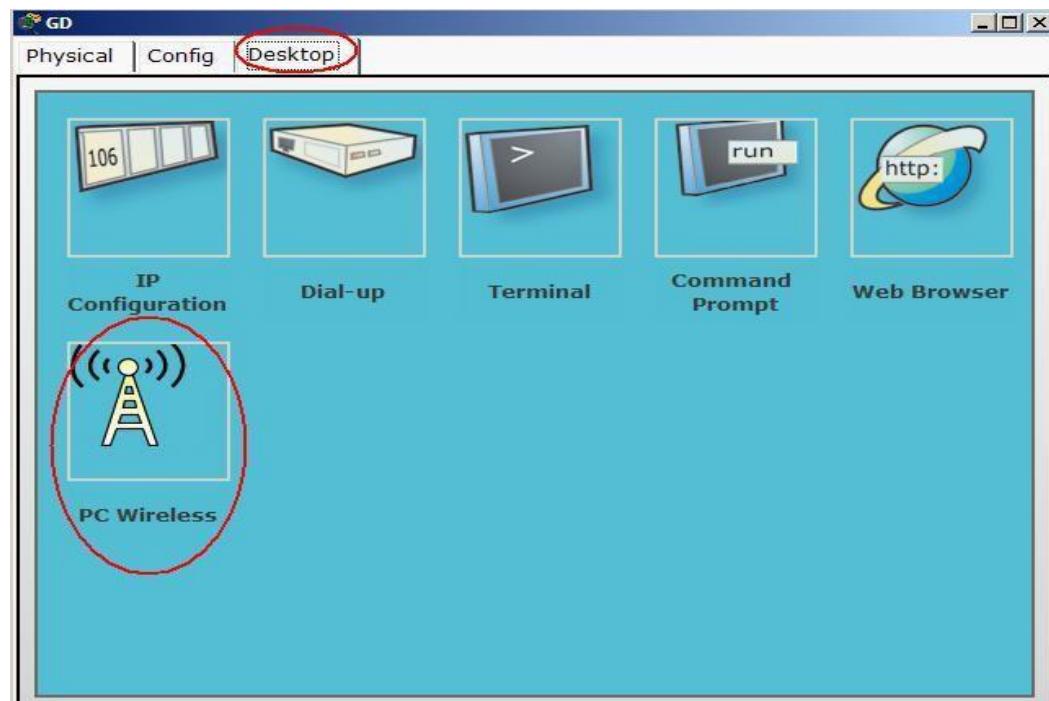


Sau khi tiến hành xong các bước trên, chúng ta tiến hành cấu hình IP và các thông số khác cho máy để có thể tiến hành connect vào mạng Wireless.

Để cấu hình IP và các vấn đề khác như bảo mật, xem các thông tin về địa chỉ Mac... thì ta chọn tab CONFIG Wireless



Ta chọn Tab DESKTOP PC Wireless như hình minh họa sau:



Nếu có hiện lên thông báo như sau thì chúng ta đã kết nối thành công vào mạng Wireless



Chúng ta có thể vào các TAB CONNECT và PROFILES để xem thêm các thông tin khác và lựa chọn các hệ thống mạng để kết nối vào.

