ĐẠI HỌC BÁCH KHOA HÀ NỘI

**TÀI LIỆU HƯỚNG DẪN THỰC HÀNH**  **MẠNG MÁY TÍNH**  **IT3080**

**(LƯU HÀNH NỘI BỘ)**

**Phiên BẢN dành cho thỰc hành Online**

**(Update 30/10/2021)**

**VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

© 2020 – HUST – SOICT

**MỤC LỤC**

[1. GIỚI THIỆU 3](#_Toc86527062)

[1.1. MỤC ĐÍCH và phẠm vi CỦA TÀI LIỆU 3](#_Toc86527063)

[1.2. MỤC TIÊU THỰC HÀNH 3](#_Toc86527064)

[1.3. THÔNG TIN CHUNG 3](#_Toc86527065)

[2. Các qui định đối với sinh viên 3](#_Toc86527066)

[3. BÀI THỰC HÀNH SỐ 1: MÃ ĐƯỜNG TRUYỀN 3](#_Toc86527067)

[3.1. Mục đích và nội dung 3](#_Toc86527068)

[3.2. Nội dung thực hành 7](#_Toc86527069)

[1.3. BÁO CÁO BÀI THỰC HÀNH SỐ 1 8](#_Toc86527070)

[4. BÀI THỰC HÀNH SỐ 2: Xây dỰng mỘt mẠng LAN 9](#_Toc86527071)

[4.1. Mục đích và nội dung 9](#_Toc86527072)

[4.2. Nội dung thực hành 14](#_Toc86527073)

[4.3 BÁO CÁO BÀI THỰC HÀNH SỐ 2 15](#_Toc86527074)

[BÀI THỰC HÀNH SỐ 3: ĐỊNH TUYẾN TĨNH TRONG MẠNG IP 15](#_Toc86527075)

[5.1. Mục đích và nội dung 15](#_Toc86527076)

[5.2. Nội dung thực hành 19](#_Toc86527077)

[5.3 BÁO CÁO BÀI THỰC HÀNH SỐ 3 27](#_Toc86527078)

[BÀI THỰC HÀNH SỐ 4: BÀI THỰC HÀNH SỐ 4: PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC UDP VÀ TCP 30](#_Toc86527079)

[6.1. Mục đích và nội dung 30](#_Toc86527080)

[6.2. Nội dung thực hành 32](#_Toc86527081)

[BÀI THỰC HÀNH SỐ 5: PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC DNS VÀ HTTP 41](#_Toc86527082)

[7.1. Mục đích và nội dung 41](#_Toc86527083)

[7.2. Nội dung thực hành 43](#_Toc86527084)

[Phụ lục 1: LÀM QUEN VỚI CÔNG CỤ WIRESHAKR 49](#_Toc86527085)

[Phụ lục 2: PHÂN TÍCH KHUNG TIN ETHERNET 57](#_Toc86527086)

[Phụ lục 3: PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC IP và ARP 66](#_Toc86527087)

[Phụ lục 4: KIỂM TRA TÌNH TRẠNG KẾT NỐI 86](#_Toc86527088)

[Phụ lục 5: HƯỚNG DẪN SỬ DỤNG PACKET TRACER 98](#_Toc86527089)

# 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: MÃ ĐƯỜNG TRUYỀN

## 3.1. Mục đích và nội dung

**3.1.1. Mục đích**

Bài thí nghiệm này được thiết kế để sinh viên làm quen với các công cụ trong giám sát mạng và trong mô phỏng.

**3.1.2. Yêu cầu đối với sinh viên**

* Môi trường thực hành:
  + Máy tính (Windows, Linux)
  + Phần mềm mô phỏng mã đường truyền (Line code simulation), phần mềm mô phỏng mạng (Cisco Packet Tracer), phần mềm phân tích dữ liệu mạng (Wireshark).
* Kiến thức: Nắm vững kiến thức về mã đường truyền, phương thức đóng gói gói tin qua từng lớp mạng trong mô hình OSI.
* 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**

Mã đường truyền là mã được chọn để sử dụng trong việc truyền thông giữa các hệ thống, cụ thể là để truyền tín hiệu số qua đường truyền. Mã đường dây thường được sử dụng trong việc truyền dữ liệu số.

Mã đường truyền biểu diễn dữ liệu số dưới dạng sóng được tối ưu cho các thuộc tính cụ thể của đường truyền vật lý (và cả thiết bị thu nhận). Các mẫu điện áp, dòng điện hoặc photon được sử dụng để biểu diễn dữ liệu số trên một liên kết truyền được gọi là mã đường truyền.

Có hai nhóm mã đường truyền chính: RZ (Return-to-Zero) và NRZ (Non-Return-to-Zero). Với mã đường truyền RZ, sóng về mức 0 khi chưa hết 1 chu kỳ bit (thường là ½ chu kỳ). Các mã đường truyền cũng có thể được phân loại dựa trên kỹ thuật gán mức tín hiệu để biểu diễn dữ liệu số, chẳng hạn như unipolar, polar, bipolar, và Manchester.

+ Mã Unipolar

Điện áp dương biểu thị giá trị nhị phân 1 và điện áp 0 volt biểu thị giá trị nhị phân 0. Đây là mã đường truyền đơn giản nhất, trực tiếp mã hóa dòng bit.

+ Mã Polar

Điện áp dương biểu thị giá trị nhị phân 1 và điện áp âm biểu thị giá trị nhị phân 0.

+ Mã Bipolar

Giá trị nhị phân 1 đươc biểu diễn bằng mức điện áp dương hoặc âm, giá trị nhị phân 0 được biểu diễn bằng mức điện áp 0. Như vậy mã Bipolar có ba giá trị là +, - và 0.

+ Mã Manchester

Giá trị nhị phân 1 đươc biểu diễn bằng mức điện áp âm đi liền sau mức điện áp dương với độ rộng mỗi mức điện áp là ½ chu kỳ, ngược lại giá trị nhị phân 0 đươc biểu diễn bằng mức điện áp dương đi liền sau mức điện áp âm với độ rộng mỗi mức điện áp là ½ chu kỳ.

A close up of text on a white surface

Description automatically generated

Biểu diễn dữ liệu số qua các loại mã đường dây

A close up of a piece of paper

Description automatically generated

+ Mã Differential

Một mã thường ứng dụng mã Manchester để kiểm tra lỗi. Trong mã này, giá trị nhị phân đầu vào được so sánh với giá trị được mã hóa, nếu khác nhau thì mức điện áp đươc biểu diễn bằng mức điện áp âm đi liền sau mức điện áp dương với độ rộng mỗi mức điện áp là ½ chu kỳ, nếu khác nhau thì ngược lại mức điện áp dương đi liền sau mức điện áp âm với độ rộng mỗi mức điện áp là ½ chu kỳ.

A screenshot of a cell phone

Description automatically generated

**3.1.2. Công cụ phân tích dữ liệu mạng Wireshark**

Wireshark là ứng dụng phân tích dữ liệu hệ thống mạng, với khả năng theo dõi, giám sát các gói tin theo thời gian thực, hiển thị báo cáo cho người dùng qua giao diện khá đơn giản và thân thiện.

**3.1.3. Công cụ mô phỏng mạng Cisco Packet Tracer**

Packet Tracer là một công cụ mô phỏng hệ thống mạng trực quan đa nền tảng được thiết kế bởi Cisco Systems, Inc có thể chạy trên cả Linux và Windows. Công cụ này cho phép người dùng tạo cấu trúc liên kết mạng và mô phỏng giả lập các mạng máy tính. Phần mềm này cho phép người dung mô phỏng cấu hình bộ router và switch của cisco, cũng như cho phép sử dụng mô phỏng trên giao diện dòng lệnh. Packet Tracer có giao diện người dùng với tính năng kéo thả các thiết bị vào mô hình, cho phép người dùng có thể thêm, xóa các mạng mô phỏng phù hợp theo ý mình.

## 3.2. Nội dung thực hành

**3.1. Mô phỏng mã đường dây**

Sinh viên tự tạo dữ liệu số và sử dụng công cụ mô phỏng để tạo mã đường truyền.

**3.2. Cài đặt và làm quen với công cụ phân tích dữ liệu mạng Wireshark**

Sinh viên cài đặt phần mềm Wireshark. Tiến hành bắt gói tin HTTP và quan sát các tiêu đề đóng gói theo chồng giao thức TCP/IP (phụ lục 1, 2, 3, 4).

**3.3. Cài đặt và làm quen với công cụ mô phỏng mạng Cisco Packet Tracer**

Sinh viên làm quen với các chức năng được tích hợp trong phần mềm (phụ lục 5).

## BÁO CÁO BÀI THỰC HÀNH SỐ 1

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:

**Câu hỏi**

Sinh viên tự chọn chuỗi dữ liệu số 32-bit và ghi lại kết quả mã đường truyền được tạo ra

|  |  |
| --- | --- |
| Dữ liệu số |  |
| Mã đường truyền  Unipolar |  |
| Mã đường truyền  Polar |  |
| Mã đường truyền  Manchester |  |
| Mã đường truyền  Differential |  |

# 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
* Phân chia mạng LAN thành các mạng VLAN

**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:
* Switch cisco 2960c / Cisco Packet Tracer
* Máy tính – 1 cái
* Kiến thức: Làm quen với Cisco IOS trên Switch cisco 2960c hoặc phần mềm PacketTracer hoặc GNS3.
* 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**

VLAN (Virtual Local Area Network) là một mạng LAN ảo. Về mặt kỹ thuật, mỗi VLAN là một miền quảng bá (broadcast domain) được tạo bởi một hay nhiều Switch.

**Các phương pháp chia VLAN**

* Port - based VLAN: chia theo cổng trên switch – VLAN tĩnh (Static VLAN): tất cả các thiết bị gắn với cổng đó phải cùng VLAN.
* MAC address based VLAN: chia theo địa chỉ MAC của thiết bị - VLAN động (Dynamic VLAN). Trong cách cấu hình này, mỗi địa chỉ MAC được đánh dấu với một VLAN xác định.
* Protocol – based VLAN: chia theo giao thức. Định nghĩa filter trên các switch, dựa trên các trường của gói tin (hay sử dụng Type, LLC, SNAP) để xác định nó thuộc VLAN nào.

**Cổng trunk**

Khi một liên kết giữa hai switch hoặc giữa một router và một switch truyền tải lưu lượng của nhiều VLAN thì cổng đó gọi là cổng trunk. Cổng trunk phải chạy giao thức đường truyền đặc biệt. Giao thức được sử dụng có thể là giao thức độc quyền ISL của Cisco hoặc IEEE chuẩn 802.1q

**Cấu hình VLAN**

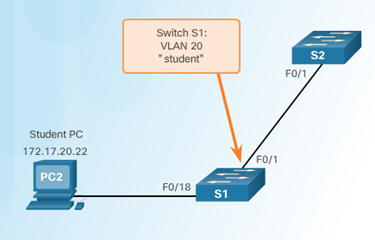
Trước tiên, chúng ta phải biết đối với thiết bị switch, có 4 kiểu hoạt động của giao diện điều khiển:

* 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.
* PRIVILEGIED 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 enbale.
* 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 conf t)
* INTERFACE CONFIG (khi hiển thị switch(config-if)#) : Kiểu này cho phép cấu hình các tham số riêng của các interfaces.

**Các lệnh tạo VLAN theo phương pháp Port - based VLAN**

* Switch# **config terminal**
* Switch(config)# **vlan** vlan-id
* Switch(config-vlan)# **name** vlan-name
* Switch(config-vlan)# **end**

Ví dụ 1: tạo VLAN có **ID**=20 và **name**=student

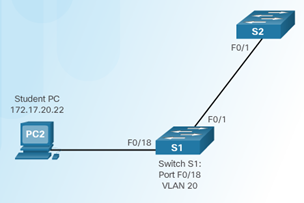


* S1# config terminal
* S1(config)# vlan 20
* S1(config-vlan)# name student
* S1(config-vlan)# end

**Các lệnh gán cổng trên switch vào VLAN**

* Switch# **config terminal**
* Switch(config)# **interface** interface-id
* Switch(config-if)# **switchport mode access**
* Switch(config-if)# **switchport access vlan** vlan-name
* Switch(config-if)# **end**

Ví dụ 2: Gán cổng F0/18 vào VLAN 20 vừa tạo ở ví dụ 1



* S1# config terminal
* S1(config)# interface F0/18
* S1(config-if)# switchport mode access
* S1(config-if)# switchport access vlan 20
* S1(config-if)# end

**Các lệnh tạo nhóm VLAN theo địa chỉ MAC**

* Switch# **config terminal**
* Switch(config)# **vlan** **database**
* Switch(config-vlan)# **map mac [mac-address][prefix-mask | host]macs-group [group-id]**
* Switch(config-vlan)# **exit**

Ví dụ 3: tạo 2 nhóm, nhóm 1 thực hiện lọc đia chỉ MAC có giá trị 0a:1b:2c:3d:4e:5f, nhóm 2 thực hiện lọc địa chỉ MAC có 32 bit đầu tiên của địa chỉ 00:11:22:33:44:55

* Switch# **config terminal**
* Switch(config)# **vlan** **database**
* Switch(config-vlan)# **map mac** 0a:1b:2c:3d:4e:5f **host macs-group 1**
* Switch(config-vlan)# **map mac** 00:11:22:33:44:55 **32 macs-group 2**
* Switch(config-vlan)# **exit**

**Gán nhóm VLAN theo địa chỉ MAC vào VLAN**

* Switch# **config terminal**
* Switch(config)# **interface** interface-id | range interface-range
* Switch(config-if)# **switchport mode general**
* Switch(config-if)# **switchport general map macs-group [group-id] vlan [vlan-id]**
* Switch(config-if)# **end**

Ví dụ 4: gán luật tạo ở ví dụ 3 vào VLAN 20 trên cổng ge1/0/12

* Switch# **config terminal**
* Switch(config)# **interface** ge1/0/12
* Switch(config-if)# **switchport mode general**
* Switch(config-if)# **switchport general map macs-group 1 vlan 20**
* Switch(config-if)# **end**

**Các lệnh tạo nhóm VLAN theo địa chỉ giao thức**

* Switch# **config terminal**
* Switch(config)# **vlan** **database**
* Switch(config-vlan)# **map protocol [protocol][encapsulation-value] protocols-group [group-id]**
* Switch(config-vlan)# **exit**

Ví dụ 5: tạo các nhóm VLAN theo giao thức có tên lần lượt là 100 và 200 để tương ứng lọc các giao thức IPv4 và IPv6

* Switch# **config terminal**
* Switch(config)# **vlan** **database**
* Switch(config-vlan)# **map ip protocols-group 100**
* Switch(config-vlan)# **map ipv6 protocols-group 200**
* Switch(config-vlan)# **exit**

**Gán nhóm VLAN theo giao thức vào VLAN**

* Switch# **config terminal**
* Switch(config)# **interface** interface-id | range interface-range
* Switch(config-if)# **switchport mode general**
* Switch(config-if)# **switchport general map protocols-group [group-id] vlan [vlan-id]**
* Switch(config-if)# **end**

Ví dụ 6: áp dụng bộ lọc VLAN giao thức có tên 100 được tạo ở ví dụ 5 vào VLAN 20 trên cổng ge1/0/20

* Switch# **config terminal**
* Switch(config)# **interface** ge1/0/20
* Switch(config-if)# **switchport mode general**
* Switch(config-if)# **switchport general map protocols-group 100 vlan 20**
* Switch(config-if)# **end**

**Các lệnh xem thông tin VLAN trên Switch**

* Switch# **show vlan** brief
* Switch# **show vlan name** student
* Switch# **show vlan** summary
* Switch# **show interfaces** **vlan** 20
* Switch# **show vlan** macs-groups
* Switch# **show vlan** protocols-groups
* Switch# **show interfaces switchport** [interface-id]

## 4.2. Nội dung thực hành

Tạo mạng có 3 mạng VLAN có tên là COMPTA, COMPTB và MAKERTING, ta thực hiện các bước như sau:

**Bước 1:** Tạo các VLAN

1. Chuyển sang mode GLOBAL CONFIG, bằng cách gõ lệnh: **config terminal**
2. Tạo ra mạng VLAN mã số 10, bằng cách gõ lệnh: **vlan** 10

(Giờ đây ta đang trong kiểu cấu hình mạng VLAN)

1. Đặt tên VLAN 10 là COMPTA bằng lệnh: **name** COMPTA
2. Thoát cấu hình VLAN bằng lệnh: **end**
3. Trở về kiểu PRIVILEGIED EXEC và hiển thị danh sách các VLAN bằng lệnh **show vlan**
4. Thực hiện các bước tương tự như trên để tạo VLAN 20 có tên là MARKETING.

**Bước 2:** thực hiện gán cổng 1 đến 3 vào VLAN COMPTA và cổng 4 đến 6 vào VLAN MARKETING

1. Chuyển sang kiểu GLOBAL CONFIG, bằng cách gõ lệnh: **config terminal**
2. Chọn cổng 1-3 với lệnh **interface range** fastEthernet 0/1 – 3
3. Cấu hình các cổng sang mode access bằng lệnh **switchport mode access**
4. Đưa 3 cổng trên vào VLAN COMPTA bằng lệnh **switchport access vlan** 10
5. Dùng lệnh **end** để trở về kiểu PRIVILEGIED EXEC

Làm tương tự với VLAN COMPTB nhưng áp dụng lọc địa chỉ MAC 00:11:00:22:00:33, áp dụng với VLAN MAKERTING áp dụng bộ lọc giao thức icmp

## 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:

Mô tả lại các bước đã thực hiện và nộp báo cáo dưới dạng file doc (yêu cầu nộp bản mềm, có chụp màn hình các thao tác đã thực hiện)

# 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:
  + Sinh viên có khả năng kết nội các thiết bị mạng switch, router để tạo thành các mạng con kết nối với nhau
  + Sinh viên thiết lập thành thạo bảng định tuyến tĩnh cho các router.
* **Nội dung cần nộp cuối buổi thực hành:**
  + Demo cho trợ giảng các bước kiểm tra kết nối cuối các phần 3.1, 3.2, 3.3. Phần demo chiếm 3 điểm/10.
  + Báo cáo (bản giấy) theo mẫu đã cung cấp. Phần báo cáo gồm các câu trả lời cho các câu hỏi, chiếm 7 điểm/10.
  + File mô phỏng sơ đồ mạng đặt tên là STT\_HọVàTên\_MSSV\_Lab03.pkt
    - Ví dụ 04\_NguyenVanAn\_20151010\_Lab03.pkt
    - Sử dụng email của SV để gửi file vào địa chỉ email: [thuchanh.it3080@gmail.com](mailto:thuchanh.it3080@gmail.com). Tiêu đề email: “Số nhóm-Bài thực hành”. Ví dụ: N01-Lab03.

**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 bít 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 28 =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 laị 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 và﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽﷽=8 bit. Nu m in Computer Engineering program, the learners should satisfy following 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 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…

|  |
| --- |
| *Cấu hình địa chỉ IP cho các máy trạm.*  Sử dụng giao diện: Desktop🡪 IP configuration của máy trạm để thiết lập địa chỉ IP, mặt nạ, gateway cho máy.  Việc thiết lập gateway cho máy thực chất là chỉ ra cho tầng IP của máy trạm rằng khi tầng này muốn chuyển một gói tin có đích không thuộc cùng mạng với máy trạm thì nó cần phải chuyển gói tin cho gateway để được xử lý tiếp. Như vậy gateway sẽ phải là router thuộc cùng mạng với máy trạm và là cửa ngõ nối với mạng bên ngoài.  *Câu lệnh cấu hình router từ CLI trên Packet tracer*.  *Câu lệnh cho phép thực hiện các lệnh ưu tiên*  Router>enable  *Câu lệnh cho phép chuyển sang chế độ cấu hình router từ dòng lệnh, mỗi lệnh một dòng.*  Router#configure terminal  *Câu lệnh này Xác định interface sẽ được cấu hình là GigabitEthernet0/1*  Router(config)#interface GigabitEthernet0/1  *Thiết lập địa chỉ IP 10.1.0.1 với mặt nạ 255.255.0.0 cho interface đang cấu hình*  Router(config-if)#ip address 10.1.0.1 255.255.0.0  *Bật interface vừa được cấu hình*  Router(config-if)#no shutdown  *Lệnh thiết lập một đường đi tĩnh trong bảng định tuyến*  Router(config)#ip route [Network] [Mask] [Nexthop]  *Ví dụ , thêm một đường đi cụ thể đến mạng 10.1.0.0 bằng cách chuyển dữ liệu đến nút mạng tiếp theo có địa chỉ 10.3.0.2 được kết nối trực tiếp với máy qua một giao diện mạng*  Router(config)#ip route 10.1.0.0 255.255.0.0 10.3.0.2  *Lệnh kiểm tra bảng định tuyến trên router*  Router#show ip route  *Lệnh kích hoạt dịch vụ DHCP server trên một router*  Router> enable  Router#configure terminal  Router(config)#ip dhcp pool Network\_10 🡨 Đặt tên cho pool cấp địa chỉ IP  Router(dhcp-config)#network 10.0.0.0 255.255.255.0  Lệnh trên tạo một pool với tên Network\_10  gồm các địa chỉ trong dải 10.0.0.0, mặt nạ 255.255.255.0  Lênh gán default gateway cho các card mạng nhận địa chỉ IP theo DHCP, do đó một  Router(dhcp-config)#default-router 10.0.0.1  *Lệnh kích hoạt dịch vụ DHCP client trên một giao diện của 1 router*  Router> enable  Router#configure terminal  Router(config)#interface FastEthernet1/1  Router(config-if)#ip address dhcp  *Lệnh kiểm tra địa chỉ IP của một giao diện trên một router*  Router#show interface FastEthernet 1/1  *Câu lệnh kiểm tra kết nối giữa các máy*  $ ping [địa chỉ IP máy đích]  *Ví dụ:*  $ ping 10.1.0.2  *Câu lệnh in đường đi của một gói tin đến một host*  $ tracert [địa chỉ IP máy đích]  *Ví dụ:*  $ tracert 192.168.205.1  *// Lệnh để lưu cấu hình Router vào startup config*  Router#copy running-config startup-config |

*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 thực hiện bài thực hành cá nhân trên máy tính được cài đặt Packet Tracer. Sinh viên tự đăng ký tài khoản cho mình.

**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 vứoi trụ sở phía bên kia. Để 2 trụ sở có thể giao tiếp với nhau, một được cáp thuê riêng (leased line) được thiết lập giữa 2 trụ sở Saigon và Hanoi.

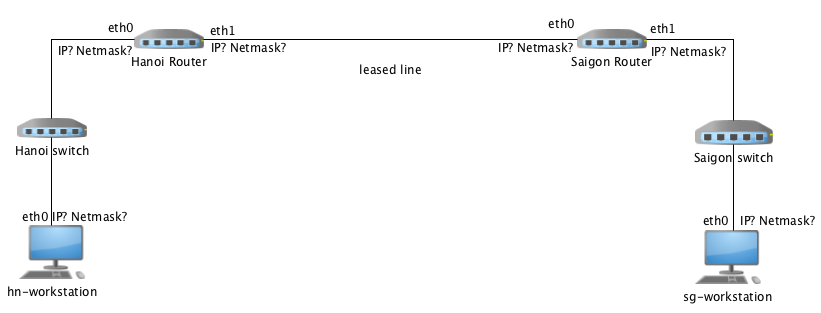
Mạng Sài gòn được cung cấp dải địa chỉ IP 10.1.0.0 với mặt nạ 255.255.0.0. Tương tự, mạng Hà nội được cung cấp dải địa chỉ IP 10.2.0.0 và cũng sử dụng mặt nạ 255.255.0.0.

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

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

**5.2.2 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: .................................GW: ...........................  Địa chỉ IP sg-workstation: ................................ Mặt nạ:..................................GW:............................  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:......................................................... |



Hình 1: Sơ đồ mạng

**5.2.3. 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 như 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*. Lưu ý chọn Router có tối thiểu 4 cổng.

**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 gateway cho máy trạm. Mặc định với mọi đích không cùng mạng với máy trạm, dữ liệu được chuyển qua gateway. Ví dụ với máy trạm hn-workstation thì gateway sẽ là Hanoi Router vì đây là cửa ngõ để đi ra các mạng khác và máy trạm cần chuyển các gói tin hướng đến mọi mạng khác qua cửa ngõ này.

**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 2 (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 3 (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:  ...............*..................................................................................................................................* .....................*...* |

**Bước 4 (1 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:~# tracert 1 10.2.0.10

tracert 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.

**5.2.4. Mở rộng mạng**

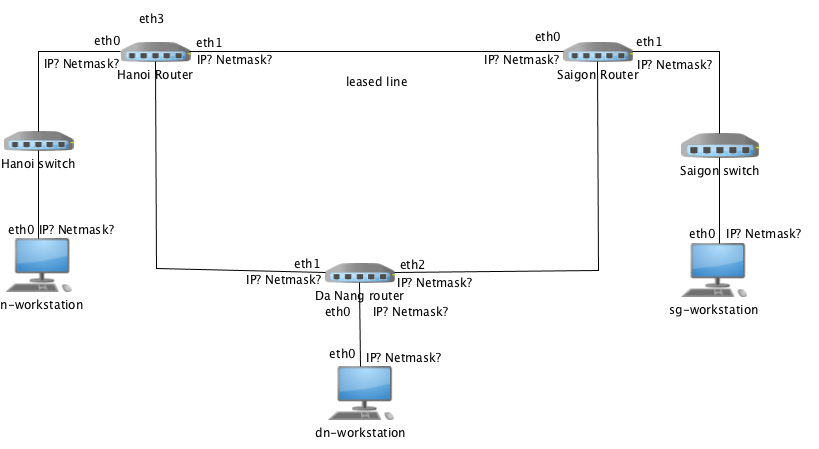
Công ty quyết định mở thêm văn phòng ở Đà nẵng. Văn phòng mới cần được kết nối với 2 văn phòng ở Hà nội và Sài gòn cũng giống như cách 2 văn phòng cũ nối với nhau. Figure 2 là sơ đồ kết nối cần đạt được. Công ty đề nghị bạn nghĩ hộ dải địa chỉ IP cần cung cấp cho mạng Đà nẵng cũng như các giao diện của các router nối với mạng này

**Bước 1**: Thực hiện kết nối các máy của văn phòng mới theo Figure 2. Cấu hình cho máy trạm của mạng Đà nẵng và router của mạng Đà nẵng để các mạng thông với nhau

|  |
| --- |
| **Câu hỏi 4 (1,5 điểm):** Gán địa chỉ IP cho mạng Đà nẵng và điền các địa chỉ lên sơ đồ mạng tại Figure 2  Địa chỉ IP của máy trạm Đà nẵng..........................................Mặt nạ:.....................................GW: ................  Địa chỉ IP router Đà nẵng-eth0..............................................Mặt nạ:.............................................................  Địa chỉ IP router Đà nẵng-eth1..............................................Mặt nạ:.............................................................  Địa chỉ IP router Hà nội –eth2..............................................Mặt nạ:.............................................................  Địa chỉ IP router Sài gòn-eth2..............................................Mặt nạ:.............................................................  Cấu hình địa chỉ IP cho máy trạm Đà nẵng  Cấu hình giao diện của router Hà nội nối với mạng Đà nẵng:  ..........................................................................................................................................................................  Cấu hình giao diện của router Sài gòn nối với mạng Đà nẵng:  ..........................................................................................................................................................................  Cấu hình các giao diện mạng của router Đà nẵng và cấu hình định tuyến để chuyển tiếp dữ liệu tới Hà Nội và Sài gòn  ..........................................................................................................................................................................  ..........................................................................................................................................................................  ……………………………………………………………………………………………………………….. |

**Bước 2**: Để router Hà nội và Sài gòn biết cách định tuyến đến mạng Đà nẵng, cần bổ sung đường đi trên router Hà nội và Sài gòn.

|  |
| --- |
| **Câu hỏi 5 (1 điểm):** Bổ sung đường đi trên router Hà nội để có thể chuyển tiếp dữ liệu đến mạng Đà nẵng  ..........................................................................................................................................................................  Bổ sung đường đi trên router Sài gòn để có thể chuyển tiếp dữ liệu đến mạng Đà nẵng  .......................................................................................................................................................................... |



Hình 2: Sơ đồ với mạng Đà nẵng

**Bước 3 (1 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, dn-workstation.

**5.25. Dịch vụ DHCP và Kết nối đến ISP**

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 3 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 eth3 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 này 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: 192.168.4.x

Netmask: 255.255.255.0

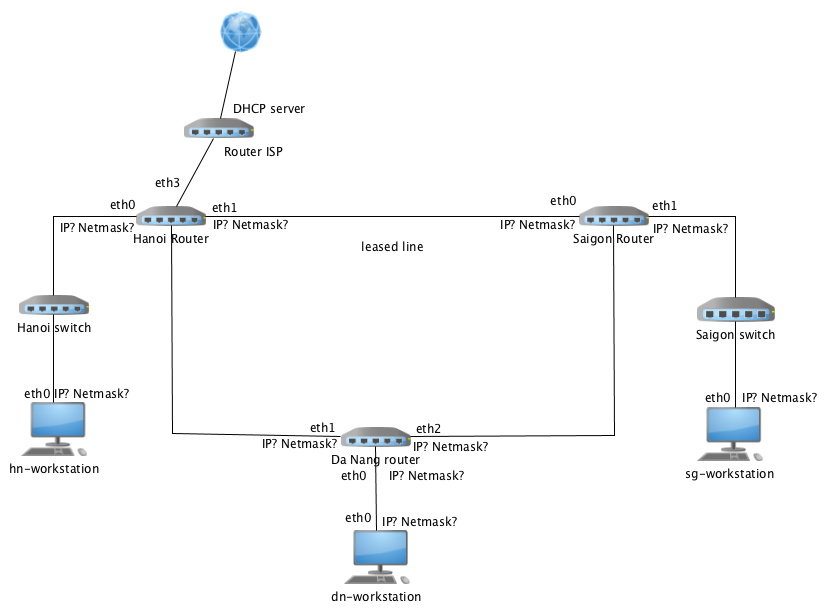
Địa chỉ IP của chính router ISP (giao diện nối với mạng Hà nội) được cố định là 192.168.4.1

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

Cụ thể các công việc cần làm như sau

**Bước 1**: 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 (0.5 điểm)**: Viết câu lệnh kích hoạt dịch vụ DHCP trên Router ISP và Router Hà nội  ..........................................................................................................................................................................  ..........................................................................................................................................................................  Địa chỉ IP mà Router Hà nội nhận được trên giao diện eth3 là gì  .......................................................................................................................................................................... |



Hình 3: Mạng với kết nối Internet tại chi nhánh Hà nội

**Bước 2**: Cấu hình router Hà nội

|  |
| --- |
| **Câu hỏi 7 (0.5 điểm)**: Điều chỉnh bảng định tuyến của router này để chuyển tiếp dữ liệu không hướng đến các mạng LAN Hà nội, Sài gòn, Đà nẵng ra Internet. Nên sử dụng đường đi mặc định  .............................................................................................................................................................................  ........................................................................................................................................... ................................. |

Mặc dù vậy các router ở Sài gòn và Đà nẵng vẫn chưa biết có thể truy cập đến các mạng ở ngoài công ty thông qua router Hà nội, vì vậy cần cập nhật bảng định tuyến của các router này.

**Bước 3**: Điều chỉnh bảng định tuyến tại các router Sài gòn, Đà nẵng

|  |
| --- |
| **Câu hỏi 8 (1 điểm)**: Điều chỉnh bảng định tuyến của router Sài gòn, Đà nẵng để chúng chuyển tiếp dữ liệu hướng đến Internet qua router Hà nội. Nên sử dụng đường đi mặc định  Điều chỉnh trên router Sài gòn:  ........................................................................................................................................................................  Điều chỉnh trên router Đà nẵng:  .........................................................................................................................................................................  Cấu hình định tuyến trên router ISP để nó có thể chuyển tiếp dữ liệu tới các mạng tại Hà Nội, Sài Gòn và Đà Nẵng.  ……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |

**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). 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, Đà nẵng, Sài gòn.

## 5.3 BÁO CÁO BÀI THỰC HÀNH SỐ 3

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:

**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

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

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

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.*

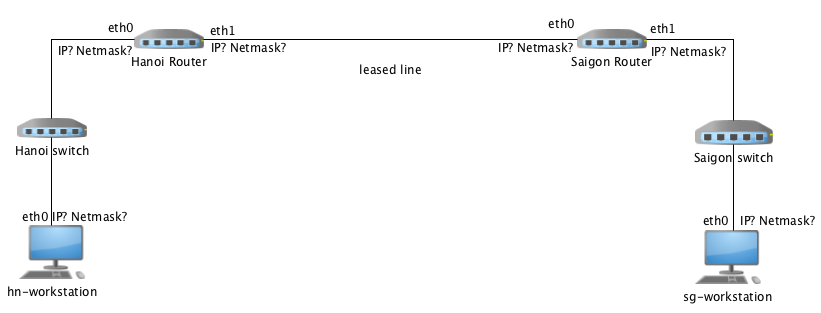


Figure 1: Sơ đồ mạng.

**Câu hỏi 2 (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 3 (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 Mở rộng mạng**

**Câu hỏi 4 (1,5 điểm):** Gán địa chỉ IP cho mạng Đà nẵng và điền các địa chỉ lên sơ đồ mạng tại Figure 2

Địa chỉ IP của máy trạm Đà nẵng ............................. Mặt nạ: ........................... GW: .................

Địa chỉ IP router Đà nẵng-eth0............................................ Mặt nạ: ............................................

Địa chỉ IP router Đà nẵng-eth1…......................................... Mặt nạ: ...........................................

Địa chỉ IP router Đà nẵng-eth2............................................. Mặt nạ: ...........................................

Địa chỉ IP router Hà nội –eth2.............................. Mặt nạ: ...........................................................

Địa chỉ IP router Sài gòn-eth2.................................Mặt nạ: ……..................................................

Cấu hình IP cho máy trạm Đà nẵng.

………………………………………………………………………………………………………………….

Cấu hình giao diện của router Hà nội nối với mạng Đà nẵng:

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

Cấu hình giao diện của router Sài gòn nối với mạng Đà nẵng:

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

Cấu hình các giao diện mạng của router Đà nẵng và cấu hình định tuyến để chuyển tiếp dữ liệu tới Hà Nội và Sài gòn.

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

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

………………………………………………………………………………………………………………..

**Câu hỏi 5 (1 điểm):** Bổ sung đường đi trên router Hà nội để có thể chuyển tiếp dữ liệu đến mạng Đà nẵng

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

Bổ sung đường đi trên router Sài gòn để có thể chuyển tiếp dữ liệu đến mạng Đà nẵng

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

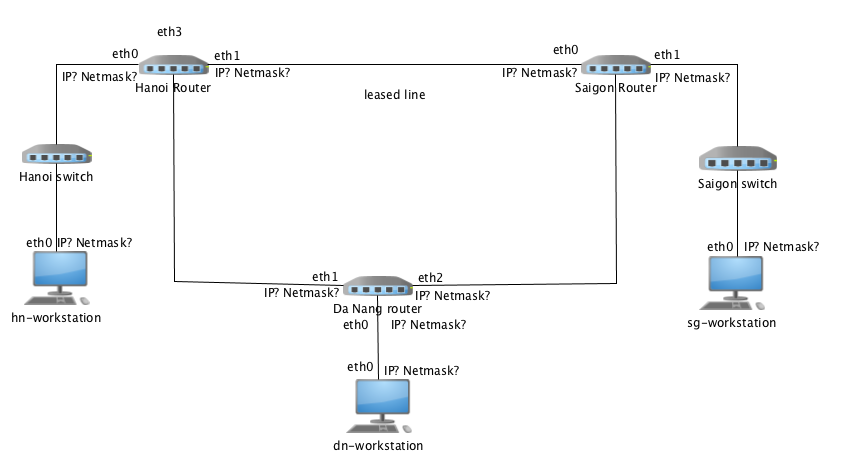


Figure 2: Sơ đồ với mạng Đà nẵng

**Câu hỏi 6 (0.5 điểm)**: Viết câu lệnh kích hoạt dịch vụ DHCP trên Router ISP và Router Hà nội

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

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

Địa chỉ IP mà Router Hà nội nhận được trên giao diện eth3 là gì

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

**Câu hỏi 7 (0.5 điểm)**: Điều chỉnh bảng định tuyến của router này để chuyển tiếp dữ liệu không hướng đến các mạng LAN Hà nội, Sài gòn, Đà nẵng ra Internet. Nên sử dụng đường đi mặc định

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

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

**Câu hỏi 8 (1 điểm)**: Điều chỉnh bảng định tuyến của router Sài gòn, Đà nẵng để chúng chuyển tiếp dữ liệu hướng đến Internet qua router Hà nội. Nên sử dụng đường đi mặc định

Điều chỉnh trên router Sài gòn:

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

Điều chỉnh trên router Đà nẵng:

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

Cấu hình định tuyến trên router ISP để nó có thể chuyển tiếp dữ liệu tới các mạng tại Hà Nội, Sài Gòn và Đà Nẵng.

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

# 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.

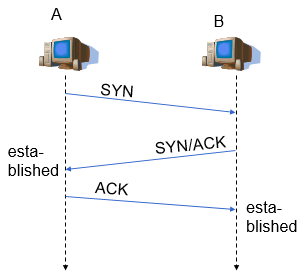
**6.1.3. Cơ sở lý thuyết**

**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 gia 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 dính 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 ngẽn 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.

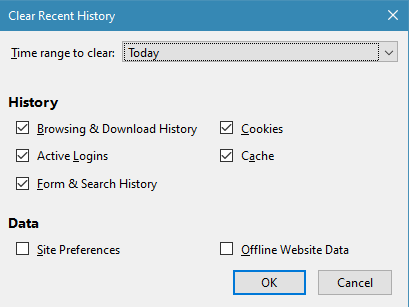
## 6.2. Nội dung thực hành

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

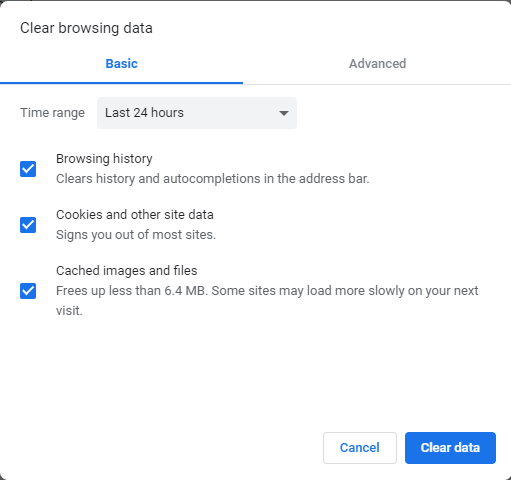
Sinh viên xác định địa chỉ IP trên máy tính ở phòng thực hành và ghi vào báo cáo. Để có được thông tin này, sinh viên xem lại bài thực hành số 2 và 3.

**6.2.2. Thu thập lưu lượng mạng**

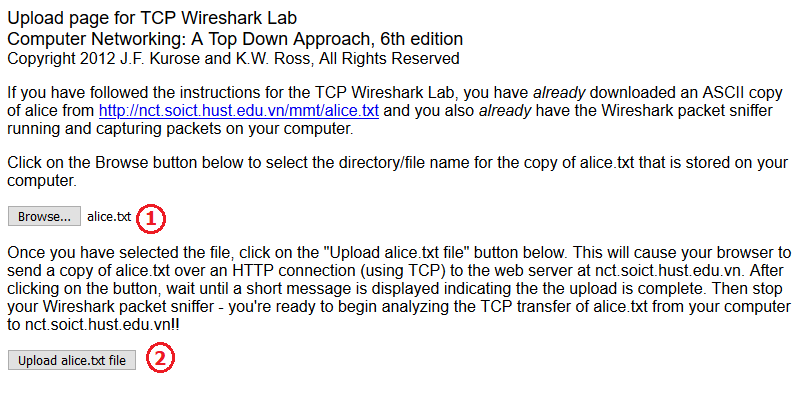
* **Bước 1:** Tắt các chương trình của người dùng có trao đổi dữ liệu trên mạng trừ trình duyệt Web để có thể quan sát quá trình truyền dữ liệu dưới đây một cách tốt nhất.
* **Bước 2:** Download file sau: [http://nct.soict.hust.edu.vn/mmt/alice.txt](http://nct.soict.hust.edu.vn/mmt/rfc793.txt)
* **Bước 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.



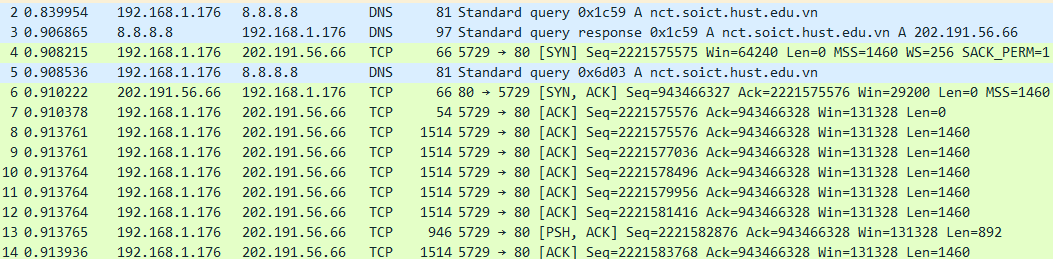
* Google Chrome: Nhấn tổ hợp phím Ctrl + Shift + Del. Chọn the past day. Chọn Cached images and files. Nhấp nút Clear data.



* **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 cạc mạng phù hợp
* **Bước 7:** Quay trở lại cửa sổ trình duyệt, upload file alice.txt đã download ở bước số 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:



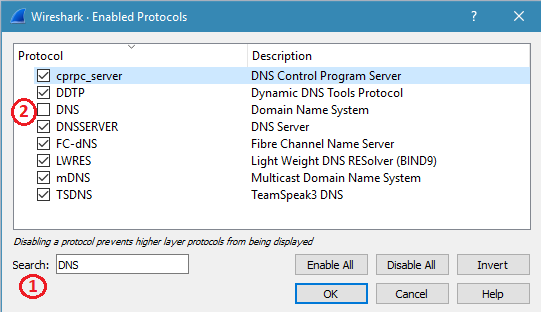
***Lưu ý:***

* *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

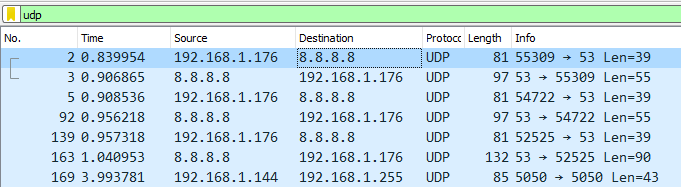
**6.2.3. Quan sát các gói tin UDP**

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.



* **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? |

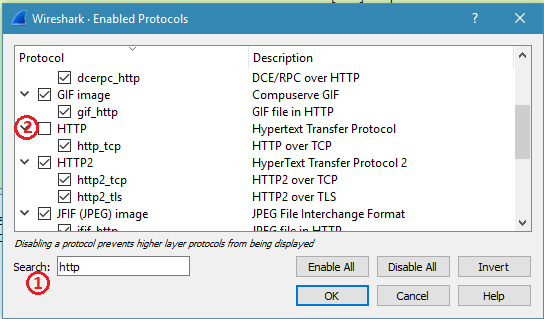
* **Bước 4:** Tìm gói tin mà máy đích trả lời cho gói tin ở bước 3 và trả lời câu hỏi 2.

|  |
| --- |
| **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? |

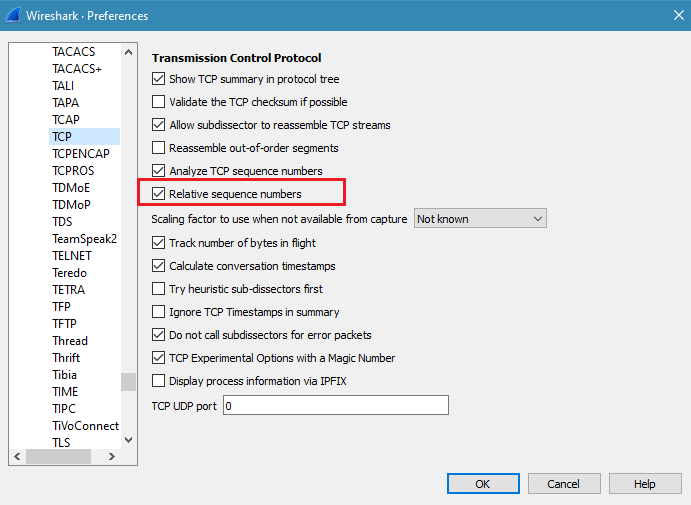
**6.2.4. Quan sát các gói tin TCP**

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.

****

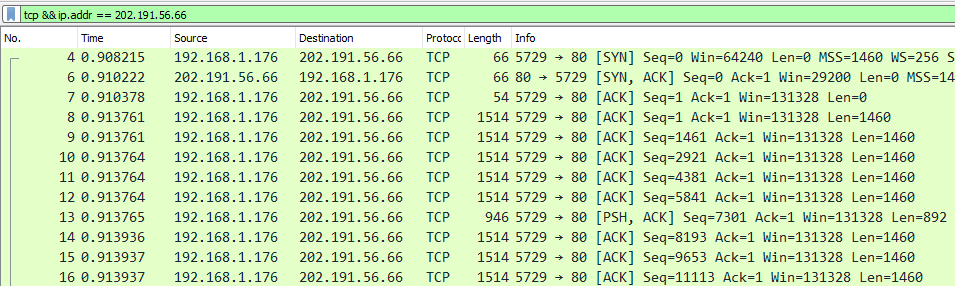
Trên menu của Wireshark, chọn **Edit 🡪 Preferences…** Trong mục **Protocol** của cửa sổ **Preference**, chọn **TCP**. Nhấn chọn mục **Relative sequence numbers** như hình sau:

****

* **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:



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

# 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, clien 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 lên kết TCP và số hiệu cổng ứng dụn 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.

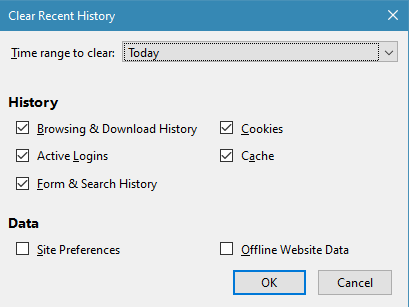
## 7.2. Nội dung thực hành

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

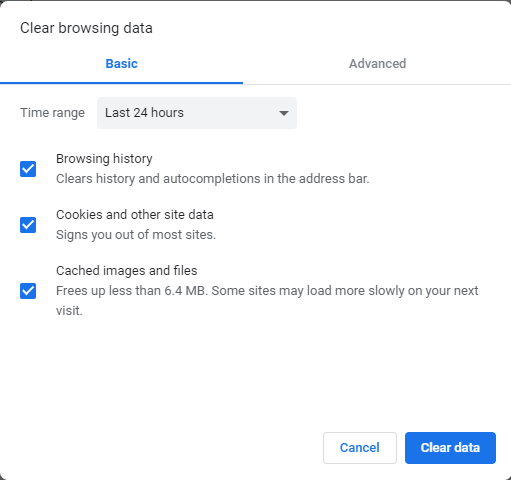
Sinh viên xác định địa chỉ IP, địa chỉ DNS Server trên máy tính ở phòng thực hành và ghi vào báo cáo. Để có được thông tin này, sinh viên xem lại bài thực hành số 2 và 3.

**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. Nhấp nút Clear data.



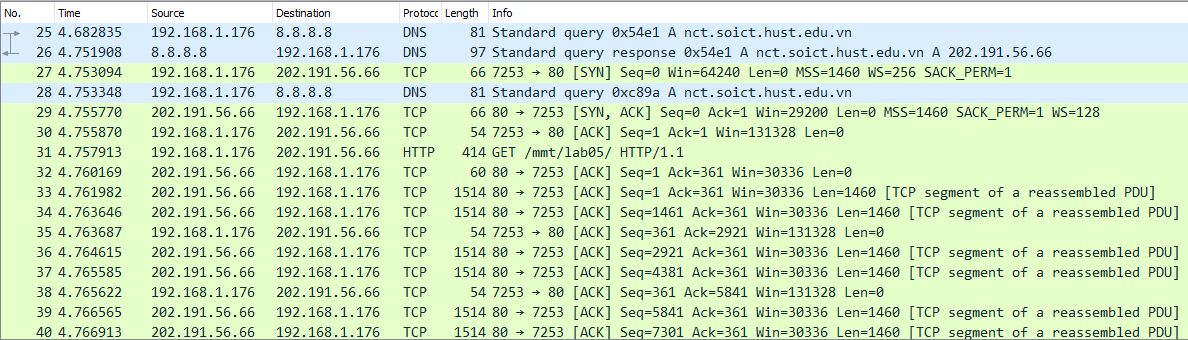
* **Bước 3:** Trên cửa sổ Command Prompt, thực hiện lệnh ipconfig /flushdns
* **Bước 4:** Khởi động phần mềm Wireshark và chọn bắt gói tin trên cạc mạng phù hợp
* **Bước 5:** Trên trình duyệt Web, mở cửa sổ duyệt riêng tư (Private Browsing):
* **Mozilla Firefox:** Nhấn tổ hợp phím Ctrl + Shift + P
*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



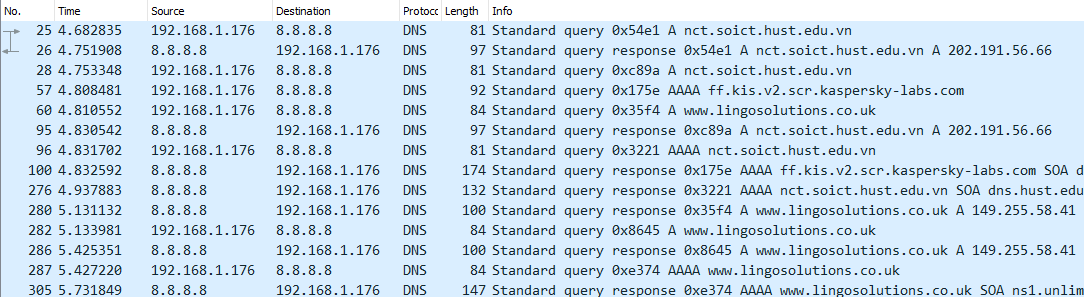
***Lưu ý:***

* *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 diệp DNS đã bắt được tương tự như hình minh họa dưới đây.



* **Bước 2:** Chọn gói tin DNS đượctrình 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? |

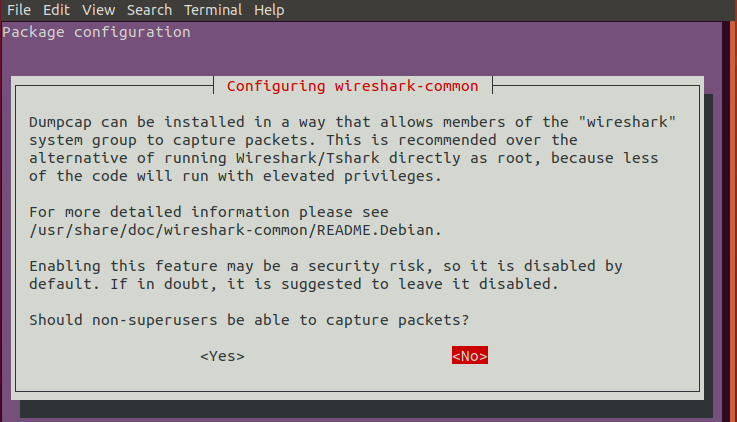
|  |
| --- |
| **Câu hỏi 9(*1 điểm*):** Đoạn sau đây mô tả ngắn gọn quá trình xử lý truy cập vào một trang Web trên trình duyệt Web. Hãy điền vào chỗ trống cụm từ còn thiếu  Khi nhận được yêu cầu truy cập vào một trang Web nào đó qua địa chỉ URL, nếu chưa biết địa chỉ IP của máy chủ Web. Trình duyệt 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. |

# 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

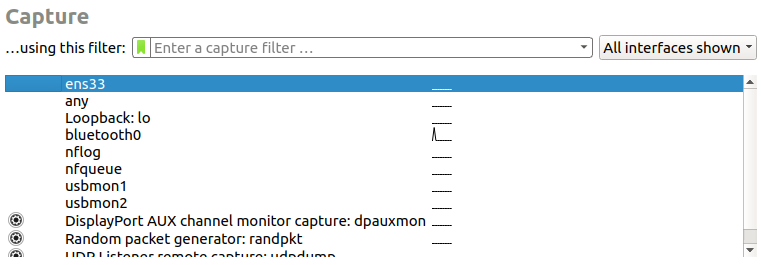
Mở cửa sổ Terminal và thực hiện lệnh **sudo apt-get install wireshark -y** để cài đặt Wireshark. Trong quá trình cài đặt, chọn No khi gặp thông báo sau:



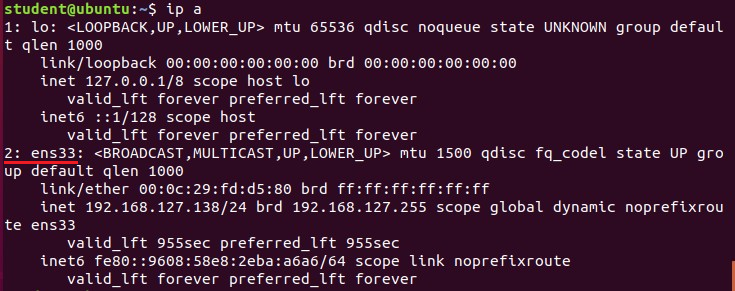
**8.1.1. Giao diện làm việc của Wireshark**

- Bước 1: Trên cửa sổ Terminal gõ lệnh **sudo wireshark** để khởi động phần mềm. Bỏ qua các cảnh báo nếu có.

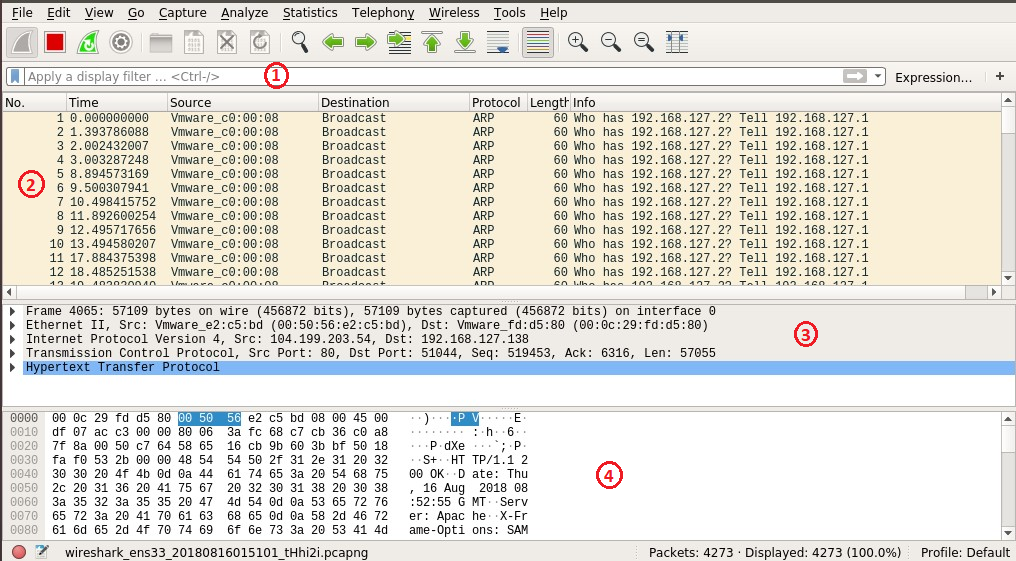
- Bước 2: Sau khi Wireshark khởi động thành công, các bạn nhìn thấy danh sách các cổng giao tiếp khác nhau trên máy tính mà Wireshark có thể bắt các gói tin trên đó.



*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



- 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

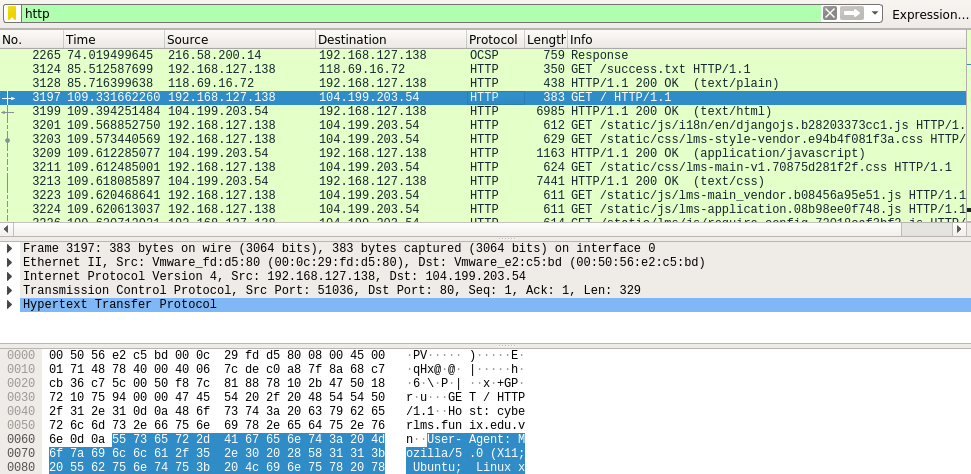
- Bước 4: Mở trình duyệt và truy cập vào trang http://cyberlms.funix.edu.vn

- 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



- 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

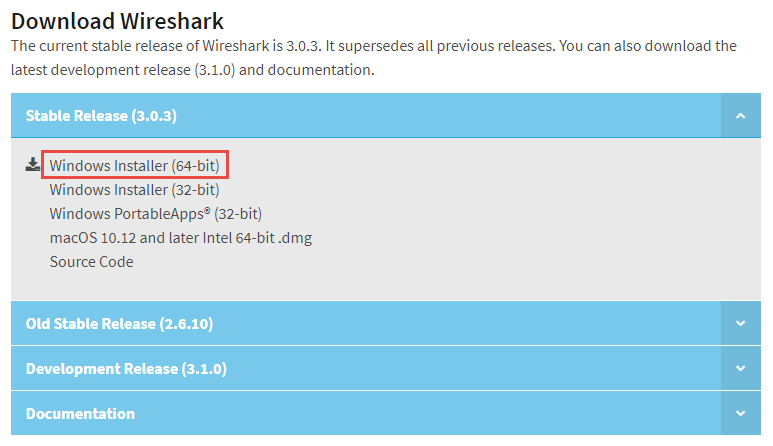
- Bước 3: Chúng ta sẽ thấy cấu trúc gói tin được hiển thị trên vùng 3, còn nội dung gói tin dưới dạng hexa và mã ASCII được hiển thị trên vùng 4. Quan sát ở vùng 3, chúng ta sẽ thấy gói tin này có các tiêu đề đóng gói theo chồng giao thức TCP/IP như sau:

* Tầng liên kết dữ liệu: Ethernet
* Tầng mạng: Internet Protocol version 4 (IPv4)
* Tầng giao vận: Tranmission 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>



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)**.

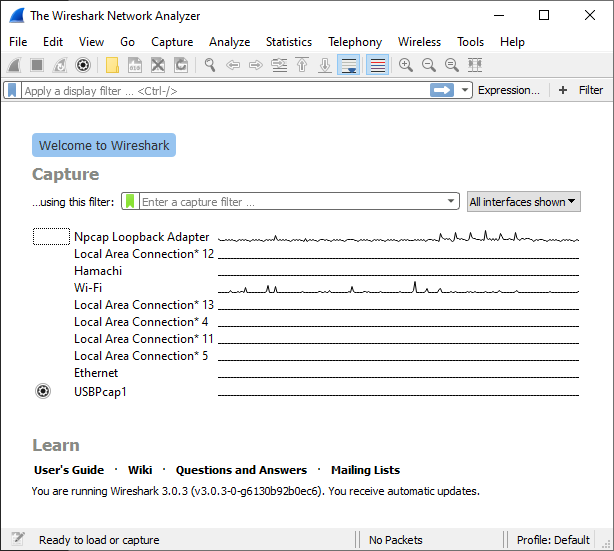
Sau khi tải về thành công, chúng ta mở tập tin ***Wireshark-win64-3.0.3.exe*** để cài đặt.



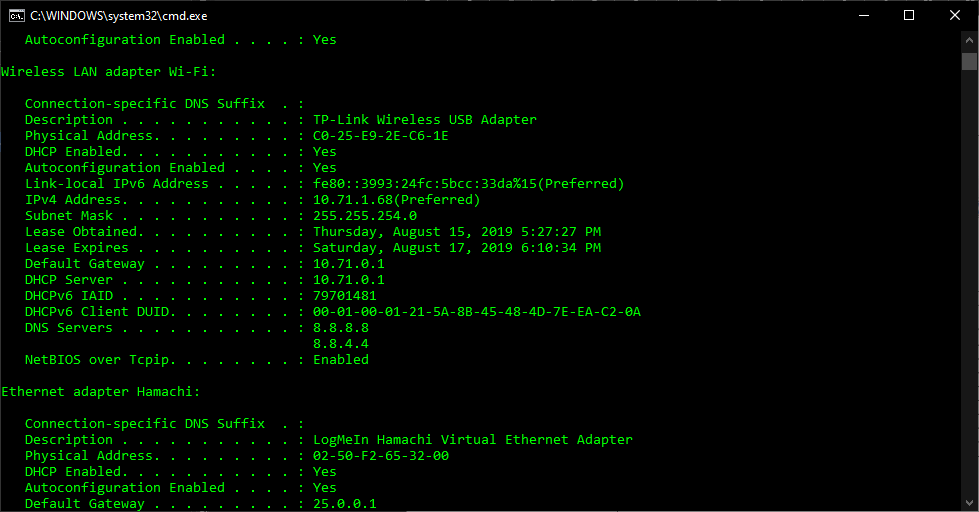
**8.2.1. Giao diện làm việc của Wireshark**

- ***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).‬‬‬‬‬‬‬‬‬‬

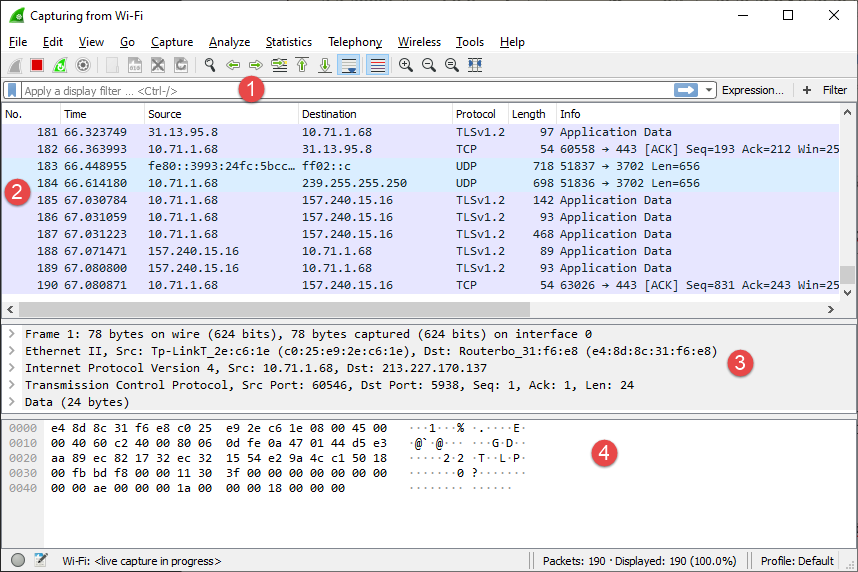
- ***Bước 2***: Sau khi Wireshark khởi động thành công, các bạn nhìn thấy danh sách các cổng giao tiếp khác nhau trên máy tính mà Wireshark có thể bắt các gói tin trên đó.



*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



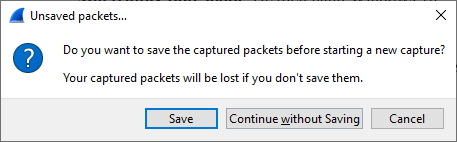
- ***Bước 3***: Nhấp đúp vào cổng mạng, chúng ta sẽ thấy giao diện làm việc của Wireshark như sau:



* 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

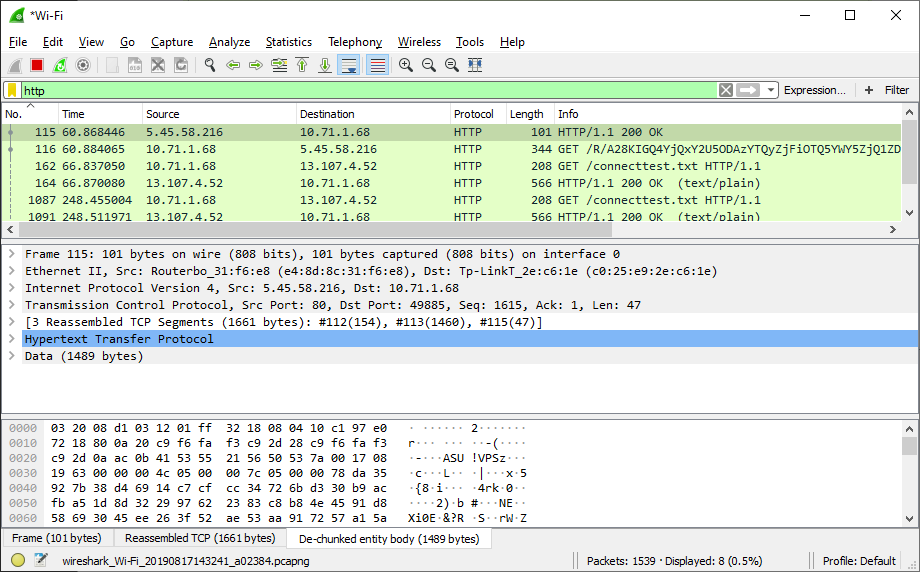
- ***Bước 5***: Ngừng bắt gói tin bằng cách nhấp vào biểu tượng  trên thanh công cụ. Chúng ta có thể lưu dữ liệu bắt được vào tệp tin có định dạng **.pcapng.**



**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.



- 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 chồng giao thức TCP/IP như sau:

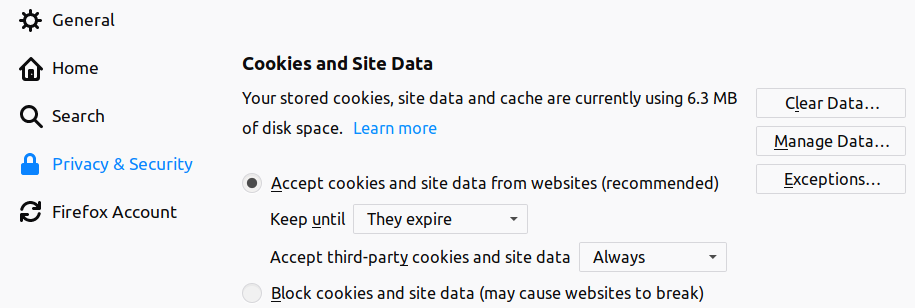
* Tầng liên kết dữ liệu: Ethernet
* Tầng mạng: Internet Protocol version 4 (IPv4)
* Tầng giao vận: Tranmission Control Protocol (TCP)
* Tầng ứng dụng: Hypertext Transfer Protocol (HTTP)

# 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**

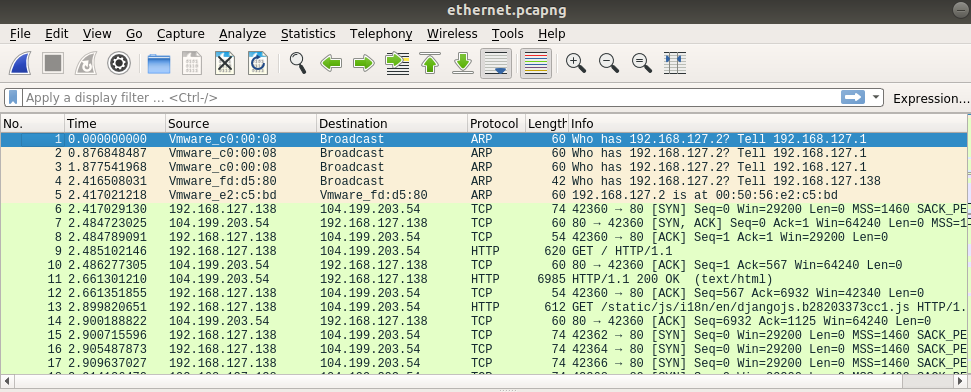
* **Bước 1**: Mở trình duyệt Firefox và xóa bộ đệm của ứng dụng như sau
* Nhấn chuột vào biểu tượng  ở góc trên bên phải
* Chọn Preferences
* Trong mục Privacy & Security, nhấn nút Clear Data



* 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 cạc mạng với Wireshark
* **Bước 4:** Mở cửa sổ Terminal thứ 2 và gõ lệnh sau:



* **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.*

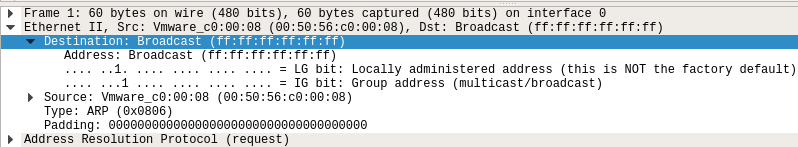
*- Các gói tin bắt được trên máy các bạn có thể sẽ có thông số khác. Điều này là hoàn toàn bình thường và không có ảnh hưởng tới quá trình thực hành*

**9.1.2. 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:*

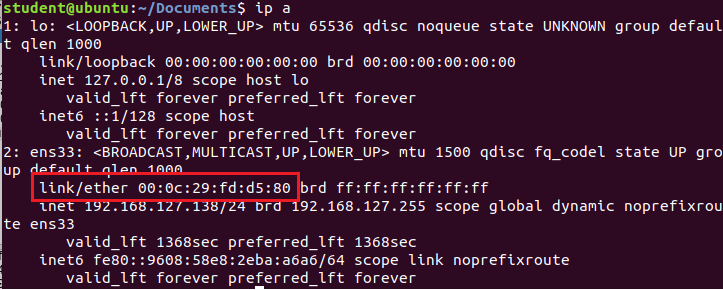
<https://drive.google.com/file/d/1Lk2PJ6m-7nmc4hJfeDoaf-V7akShVchz>

* **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:

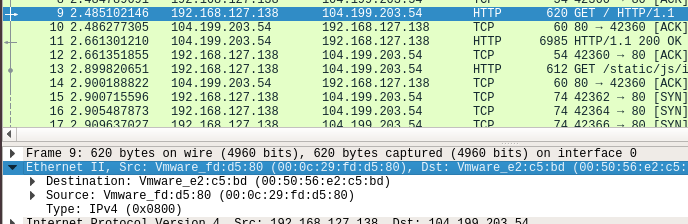


Trong kết quả minh họa trên, ta thấy cạc mạng số 2 là ens33 có địa chỉ MAC là 00:0c:29:fd:d5:80. Đối chiếu với trường Source trong tiêu đề Ethernet của gói tin trên, ta có thể thấy đây chính là giá trị của trường đó. Như vậy gói tin quảng bá mà chúng ta vừa phân tích được gửi đi trên chính máy tính này.

* **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.



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.

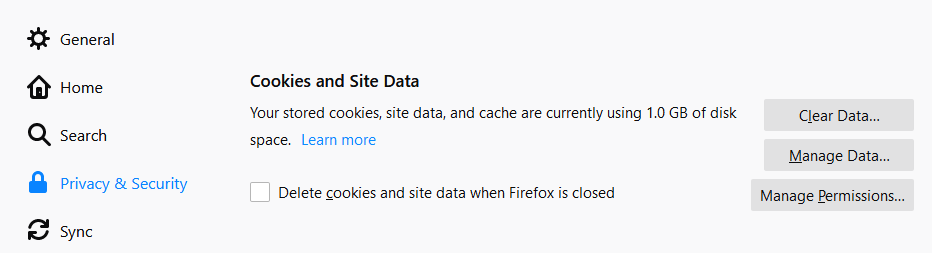
Chúng ta có thể để ý thêm phần nội dung của gói tin có xâu “GET / HTTP/1.1” và “nct.soict.hust.edu.vn”. Đây chính là dữ liệu của dịch vụ Web. Trong các bài học sau, chúng sẽ phân tích rõ hơn.

* **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.

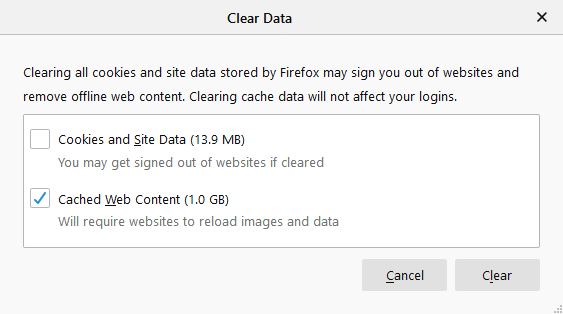
**9.2. Phân tích khung tin Ethernet trên Windows**

**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.*



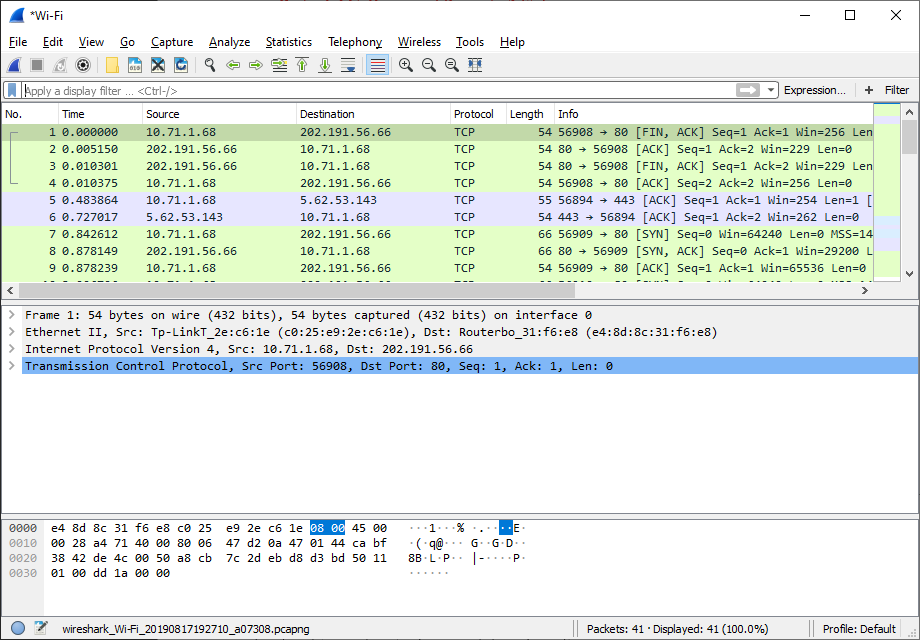
* Chọn mục *Cached Web Content* và nhấn nút *Clear.*



* ***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:



* **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.*

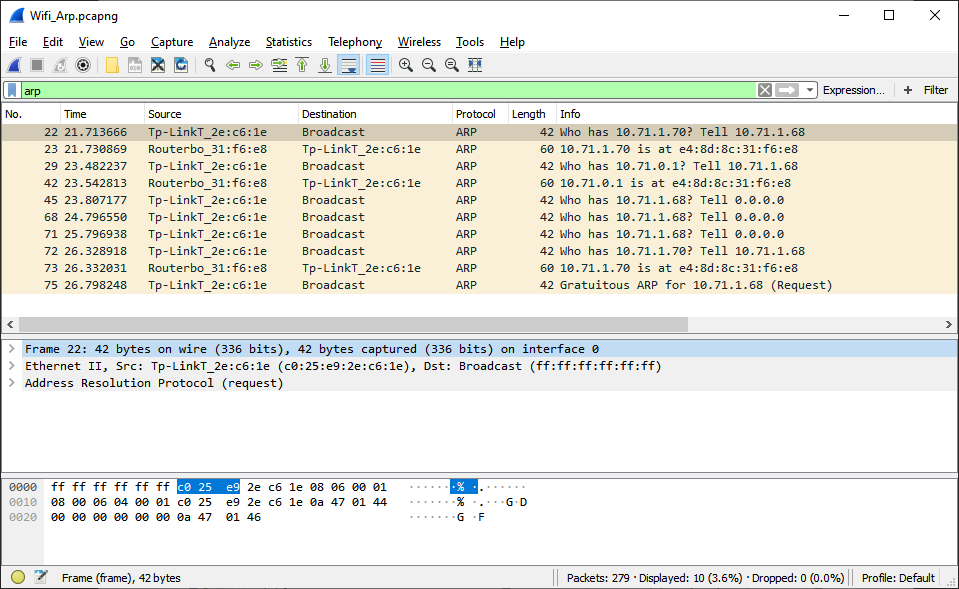
*- Các gói tin bắt được trên máy các bạn có thể sẽ có thông số khác. Điều này là hoàn toàn bình thường và không có ảnh hưởng tới quá trình thực hành.*

**9.2.2. Phân tích lưu lượng**

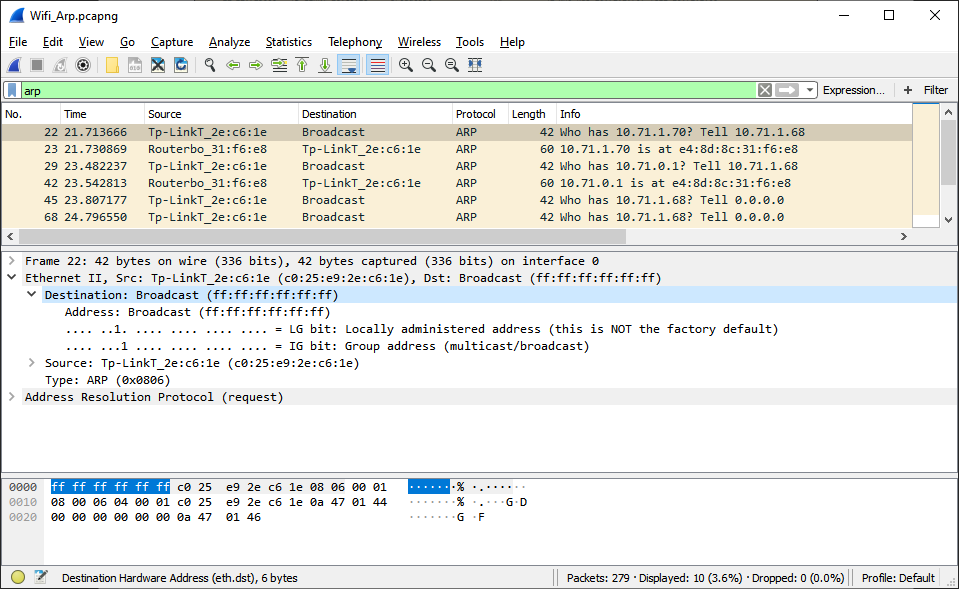
*Lưu ý: Các giá trị phân tích dưới đây chỉ mang tính chất minh họa. Với lưu lượng bắt trên máy sinh viên, kết quả có thể sẽ khác. Các bạn có thể download file lưu lượng mẫu tại địa chỉ sau cho nội dung minh họa dưới đây:*

<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).

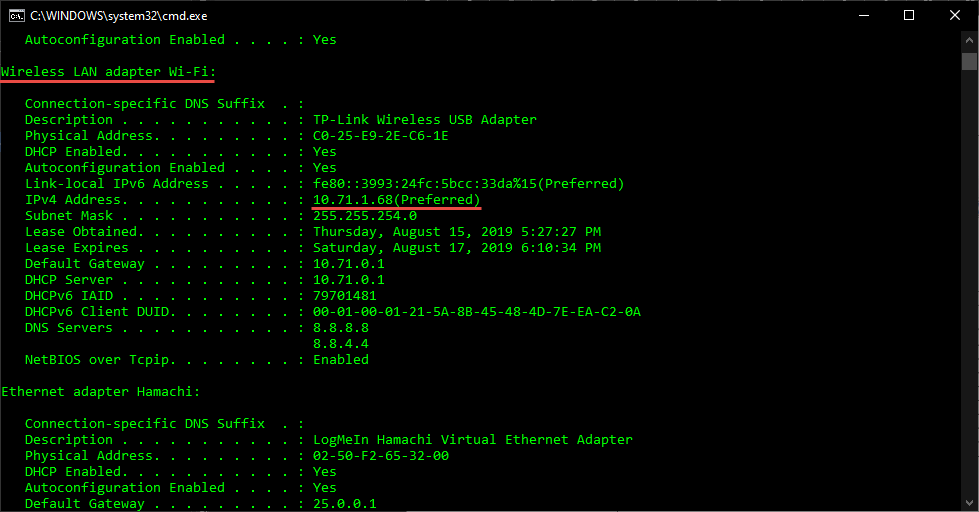


* **Bước 2**: Mở rộng phần tiêu đề Ethernet II như sau:



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:

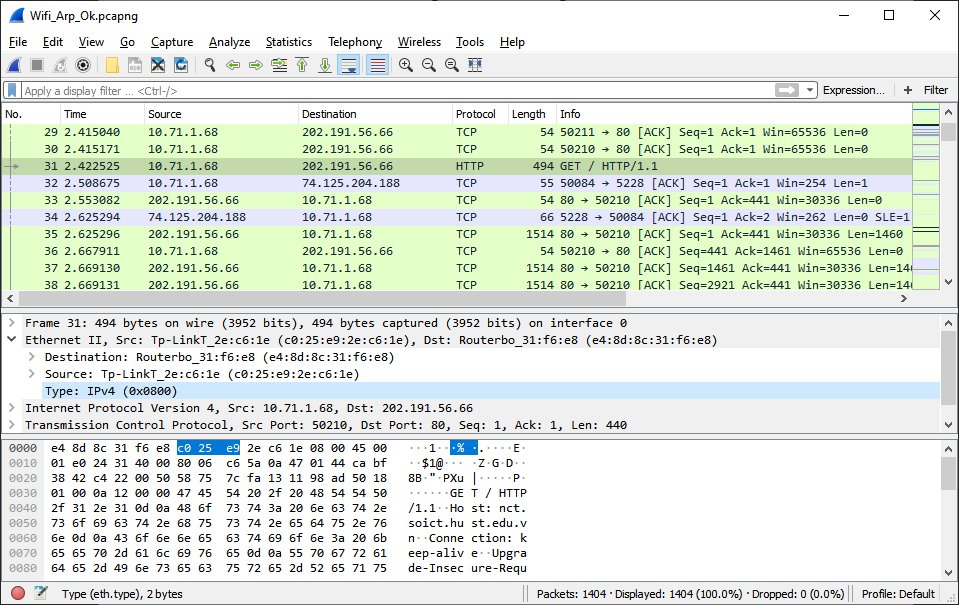


Trong kết quả minh họa trên, ta thấy cạc mạng Wireless LAN adapter Wi-Fi là TP-Link Wireless Wireless USB Adapter có địa chỉ MAC là C0-25-E9-2E-C6-1E. Đối chiếu với trường Source trong tiêu đề Ethernet của gói tin trên, ta có thể thấy đây chính là giá trị của trường đó. Như vậy gói tin quảng bá mà chúng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

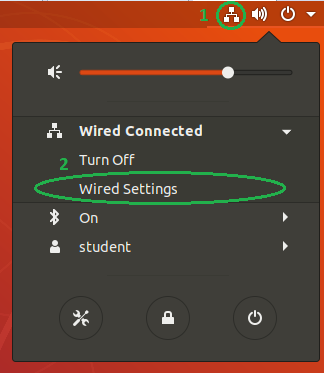
* ***Bước 6***: Chọn gói tin mà máy chủ nct.soict.hust.edu.vn gửi lại cho máy tính của chúng ta và thực hiện các bước phân tích tương tự trên. Các bạn có thể tự luyện tập để xác định các thông số trên tiêu đề Ethernet II của gói tin.

# Phụ lục 3: PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC IP và ARP

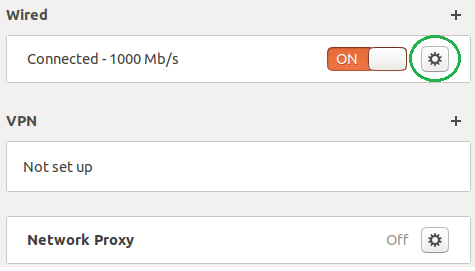
**10.1. Phân tích hoạt động trên môi trường Ubuntu**

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

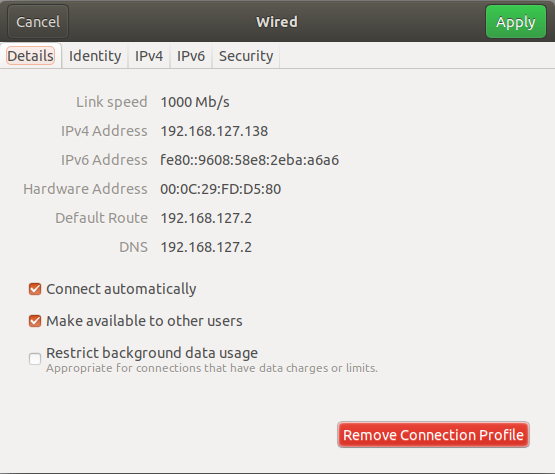
- **Bước 1:** Để không làm gián đoạn kết nối mạng của máy trạm, trước tiên ta tìm xem máy trạm đang sử dụng địa chỉ IP nào.Chọn biểu tượng kết nối mạng ở góc trên bên phải của màn hình. Chọn tiếp mục Wired Settings



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



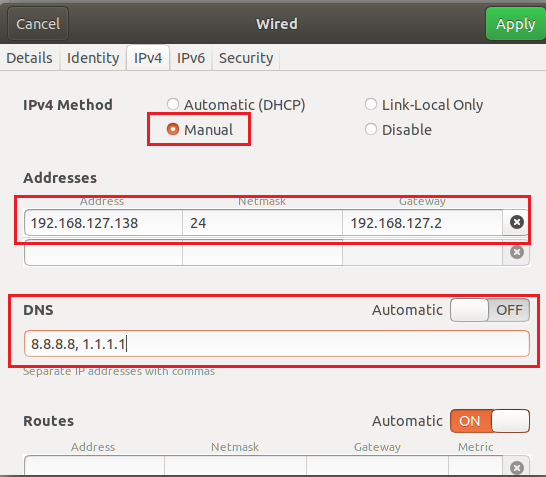
- **Bước 3**: Chúng ta có thể thấy các thông số địa chỉ IP mà máy tính đang sử dụng. Ví dụ minh họa như hình dưới đây.



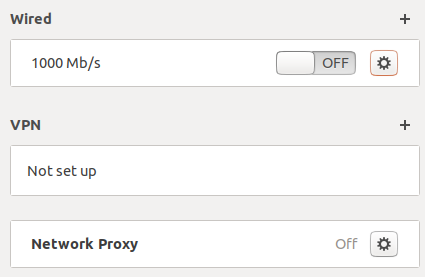
Các thông số này bao gồm:

* 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. Dễ 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

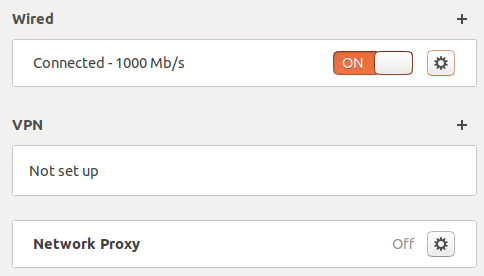
- **Bước 4**: Chọn mục IPv4 của cửa sổ trên và điền các thông số mà chúng ta đã thấy ở bước trên như sau. Nhấn nút Apply sau khi đã thiết lập xong



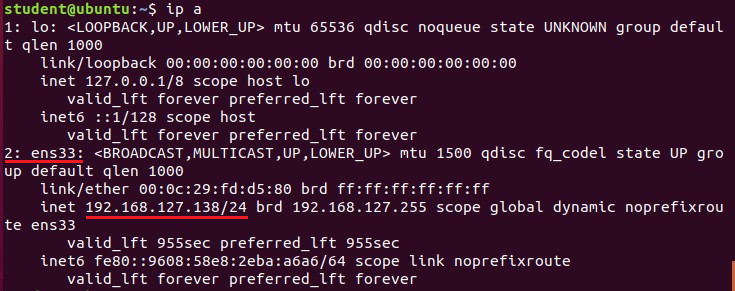
- **Bước 5:** Gạt nút ON/OFF sang vị trí OFF.



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:



- **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**

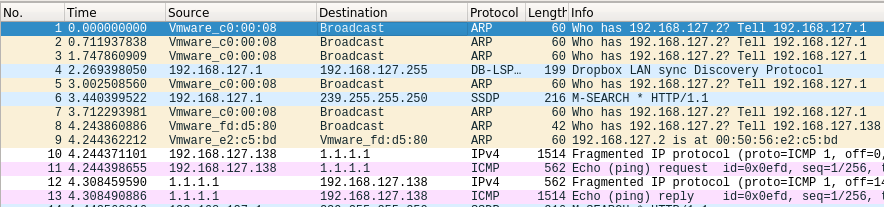
* **Bước 1:** Khởi động công cụ Wireshark từ cửa sổ Terminal với lệnh **sudo wireshark**
* **Bước 3**: Bắt đầu bắt gói tin trên cạc mạng phù họp với Wireshark
* **Bước 4:** Mở cửa sổ Terminal thứ 2 và gõ lệnh sau để xóa bảng ARP Table của máy trạm:



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



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:



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



***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.*

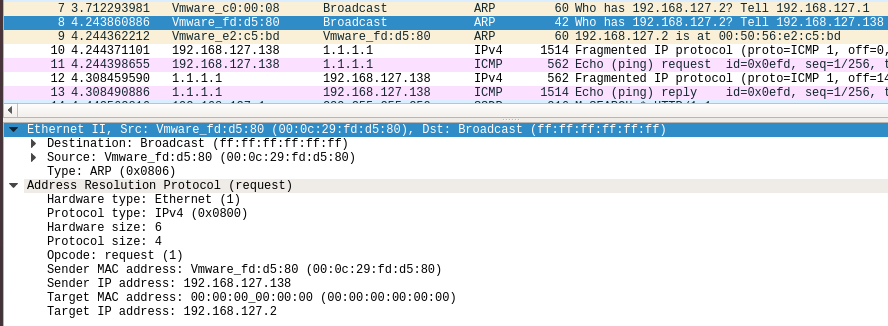
*- Các gói tin bắt được trên máy các bạn có thể sẽ có thông số khác. Điều này là hoàn toàn bình thường và không có ảnh hưởng tới quá trình thực hành*

**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:*

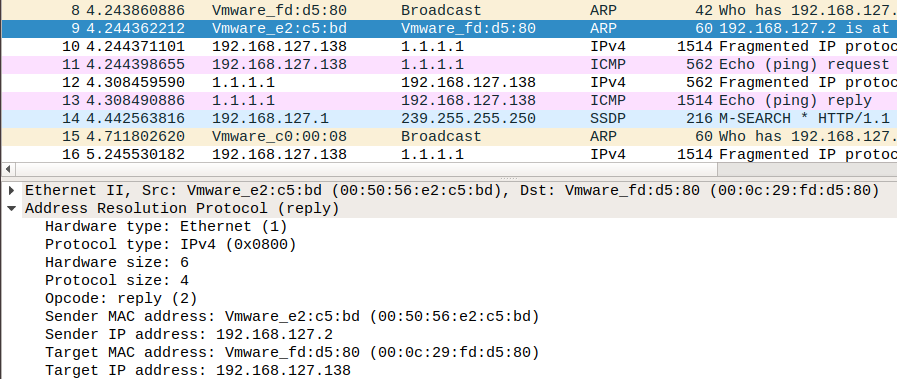
*https://drive.google.com/file/d/1iFg6Y3sk5fS1tC3FdtGHPVPlQhfI3y4Z*

* **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 đích máy của bạn. Mở rộng phần tiêu đề Address Resolution Protocol, chúng ta có thể thấy đây là gói tin ARP Request.

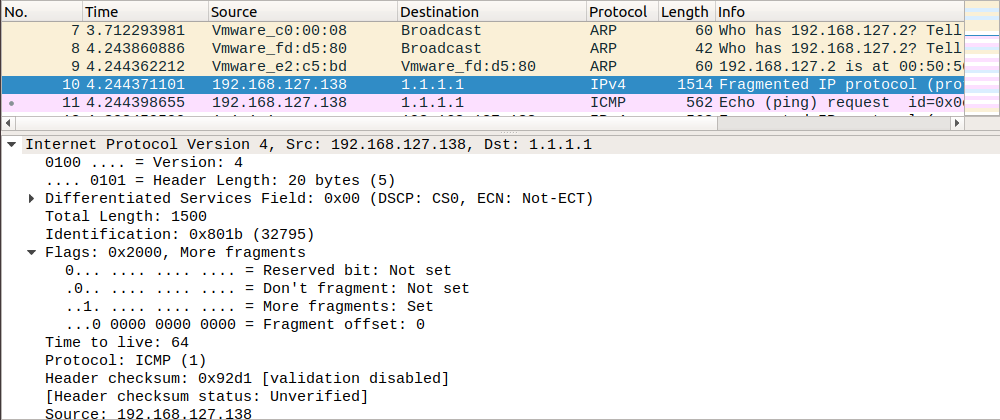


Các thông tin chúng ta đọc được từ phần tiêu đề này gồm có:

* 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.

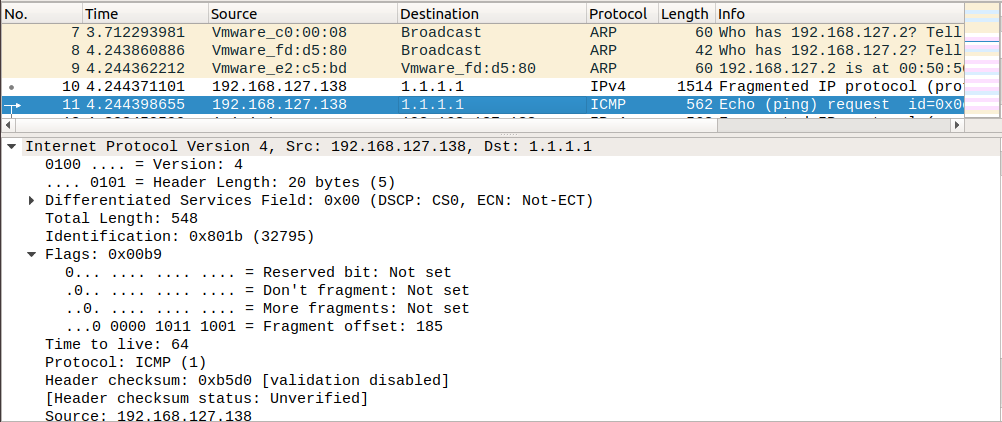


* **Bước 3**: Tìm đến gói tin đầu tiên có địa chỉ nguồn là địa chỉ IP của máy trạm mà chúng ta đã thiết lập ở trên, địa chỉ đích là 1.1.1.1



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

* Version (phiên bản): 4
* Header Length (kích thước tiêu đề): 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)
* Mỏe 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



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:

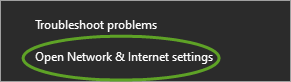
* Identification: 0x801b trùng với gói trên. Như vậy đây là một mảnh cùng một gói tin với mảnh trên.
* Flags:
* Don’t fragment: gói tin được phép phân mảnh (giá trị là 0)
* More fragments: không còn các mảnh khác (giá trị là 0)
* Fragment offset = 185 cho thấy đây là mảnh tiếp theo

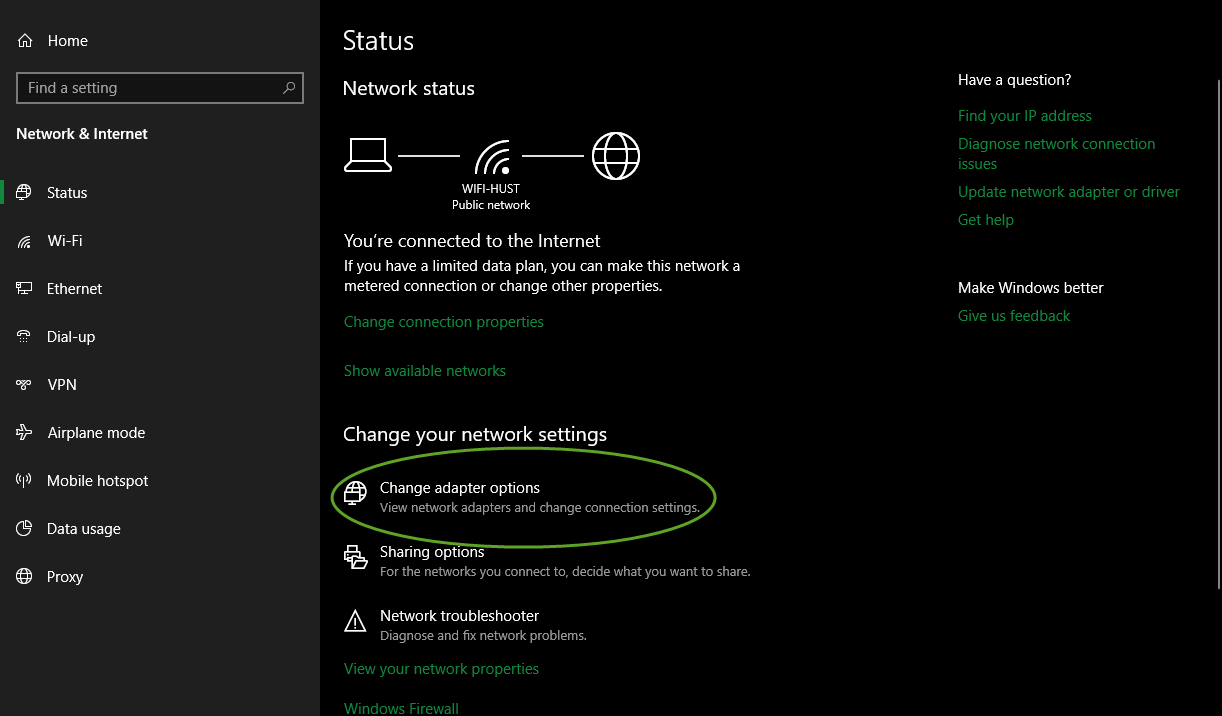
**10.2. Phân tích hoạt động trên Windows**

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

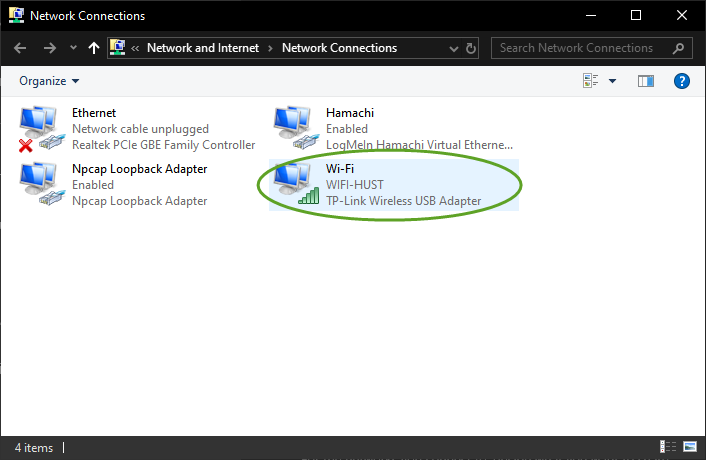
- **Bước 1 (vào phần cài đặt mạng):** Để không làm gián đoạn kết nối mạng của máy trạm, trước tiên ta tìm xem máy trạm đang sử dụng địa chỉ IP nào. Nhấn chuột phải biểu tượng kết nối mạng ở góc dưới bên phải của màn hình, chọn mục ***Open Network & Internet settings***, ở cửa sổ mới chọn tiếp mục ***Change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





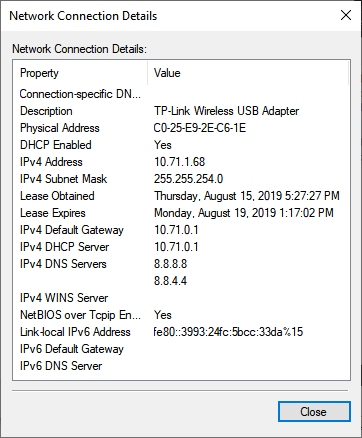


- **Bước 2 (xem thông tin mạng – nếu có)**: Nhấn đúp vào biểu tượng ***Wi-Fi*** mở cửa sổ **Wi-Fi Status**, chọn ***Details***





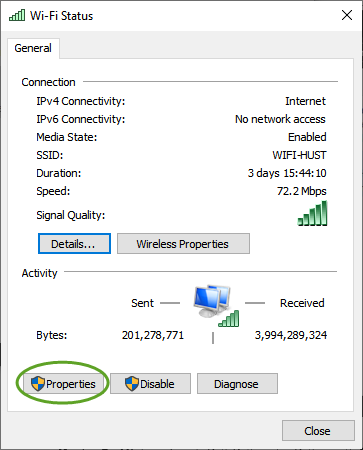
- **Bước 3 (thông tin kết nối mạng)**: Chúng ta có thể thấy các thông số địa chỉ IP mà máy tính đang sử dụng. Ví dụ minh họa như hình dưới đây:

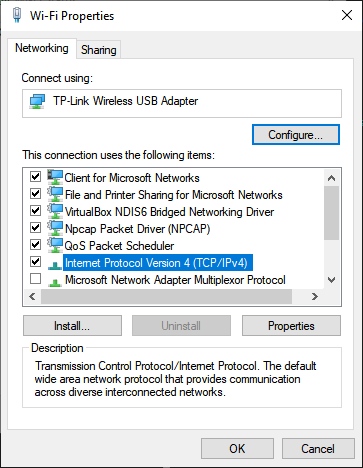


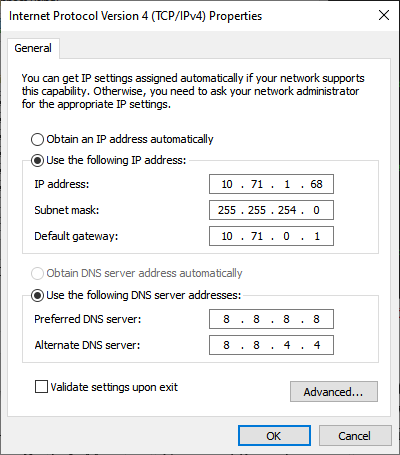
Các thông số này bao gồm:

* 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. Dễ 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

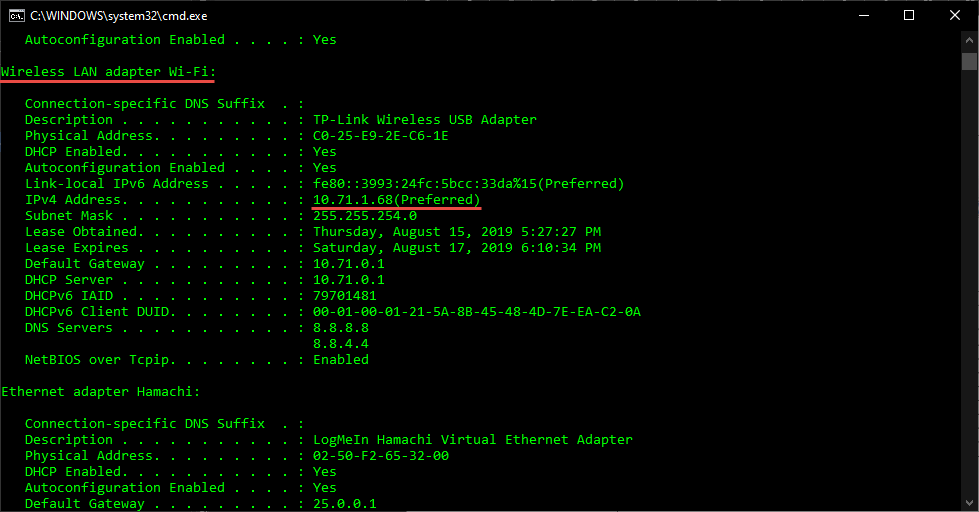
- **Bước 4 (cấu hình IP bằng tay)**: Chọn ***Close*** đóng cửa sổ hiện tại. Ở cửa sổ ***Wi-Fi Status***, chọn ***Properties*** rồi chọn ***Internet Protocol (TCP/IPv4)*** Chọn mục IPv4 của cửa sổ trên và điền các thông số mà chúng ta đã thấy ở bước trên như sau. Nhấn nút ***OK*** sau khi đã thiết lập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



- **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**

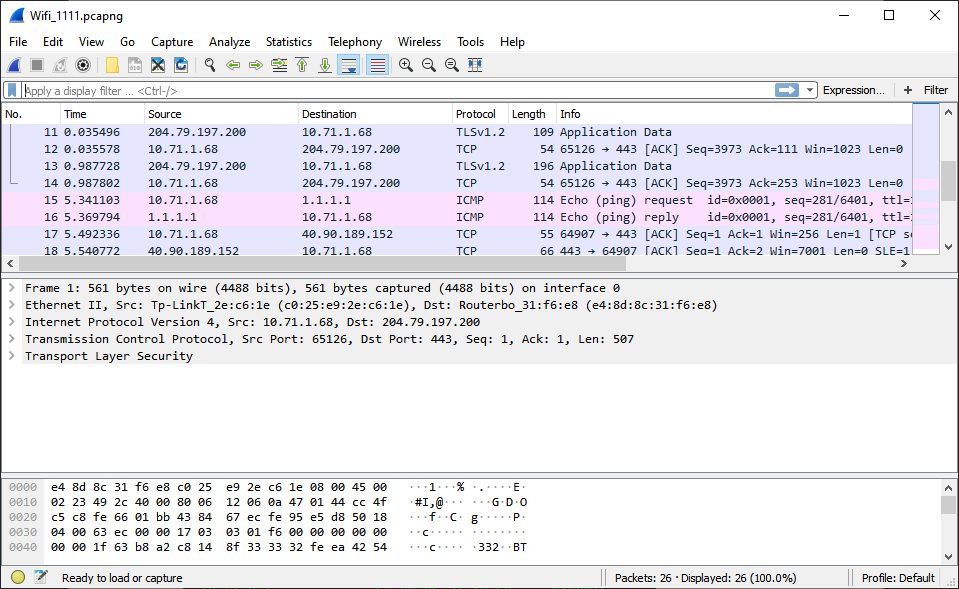
* **Bước 1:** Mở Windows Explorer vào đường dẫn cài đặt, khởi động Wireshark (ví dụ đường dẫn mặc định là: C:\Program Files\Wireshark\Wireshark.exe).‬‬‬‬‬‬‬‬‬‬‬‬
* **Bước 2**: Bắt đầu bắt gói tin trên cạc mạng phù hợp với Wireshark.
* **Bước 3:** Mở cửa sổ Command Prompt với quyền quản trị Administrator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



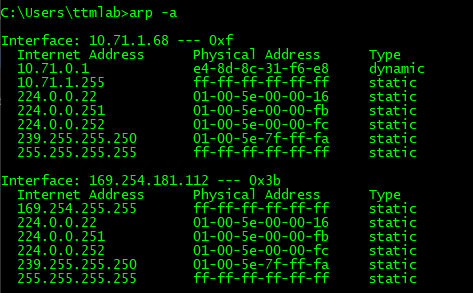
* **Bước 5:** Trên cửa số Command Prompt thực hiện lệnh ping 1.1.1.1 -s 4 -c 4 như sau:



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:



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



***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.*

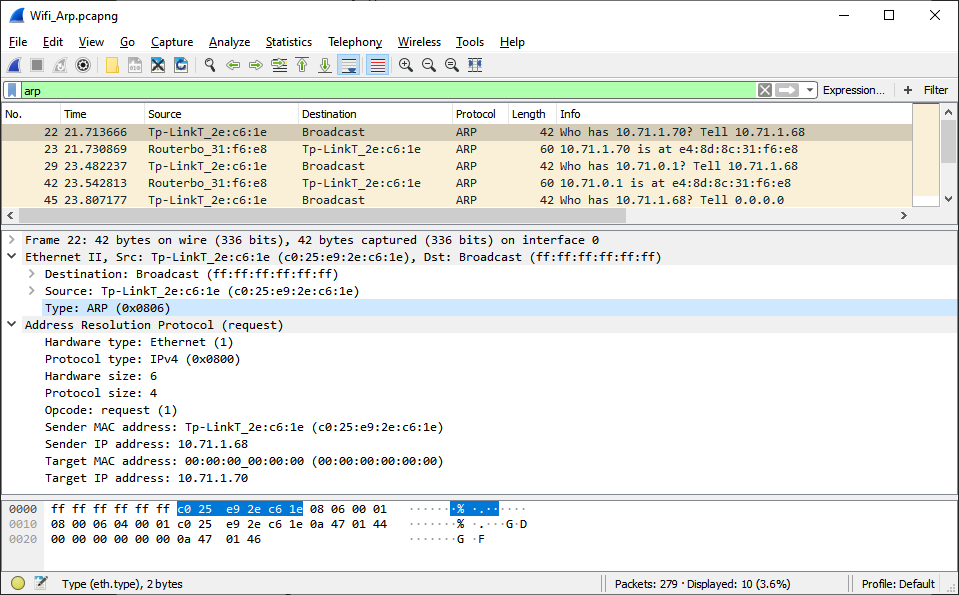
*- Các gói tin bắt được trên máy các bạn có thể sẽ có thông số khác. Điều này là hoàn toàn bình thường và không có ảnh hưởng tới quá trình thực hành.*

**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:*

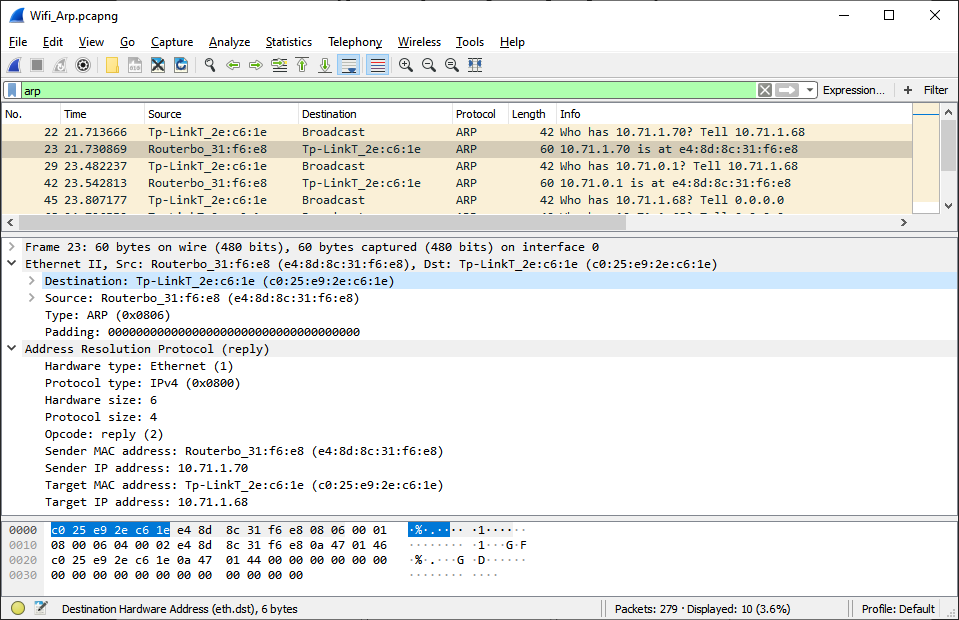
[*https://drive.google.com/file/d/1iFg6Y3sk5fS1tC3FdtGHPVPlQhfI3y4Z*](https://drive.google.com/file/d/1iFg6Y3sk5fS1tC3FdtGHPVPlQhfI3y4Z)

* **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 đích máy của bạn. Mở rộng phần tiêu đề ***Address Resolution Protocol***, chúng ta có thể thấy đây là gói tin ARP Request.

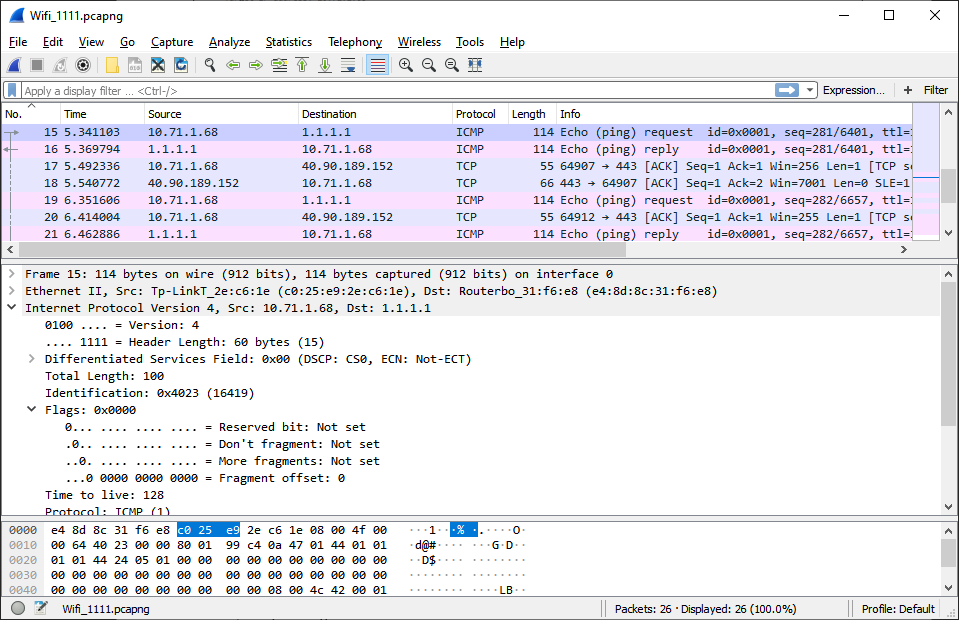


Các thông tin chúng ta đọc được từ phần tiêu đề này gồm có:

* 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.

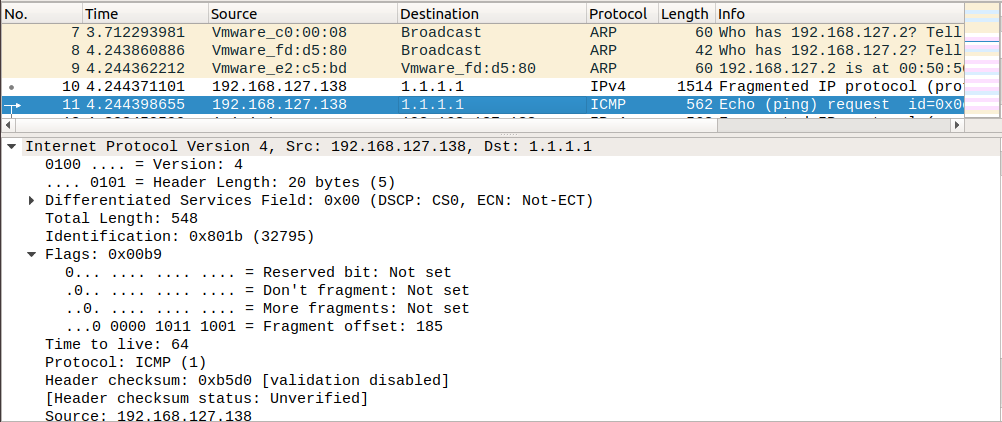


* **Bước 3**: Tìm đến gói tin đầu tiên có địa chỉ nguồn là địa chỉ IP của máy trạm mà chúng ta đã thiết lập ở trên, địa chỉ đích là 1.1.1.1



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



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

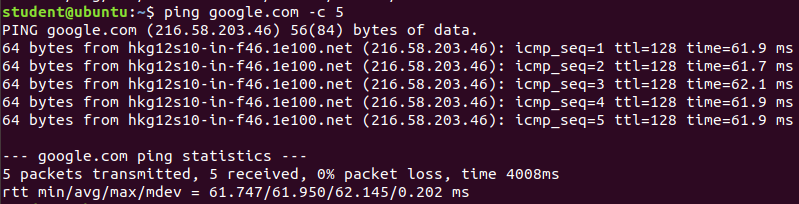
# Phụ lục 4: KIỂM TRA TÌNH TRẠNG KẾT NỐI

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

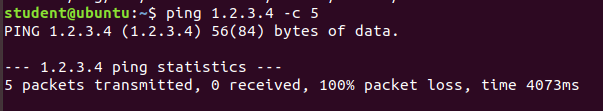
**11.1.1. Sử dụng công cụ ping**

*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.*

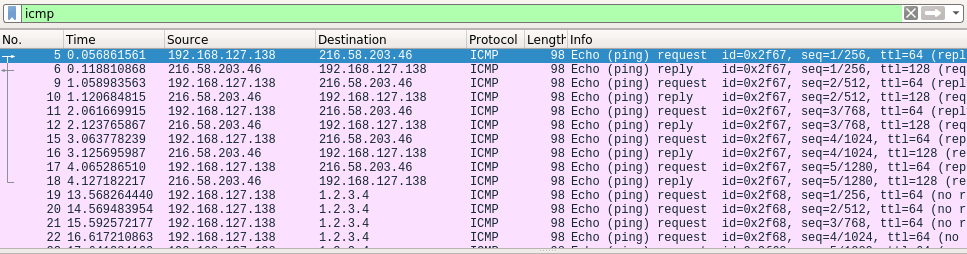
* **Bước 1**: Mở Wireshark bằng lệnh **sudo wireshark** trên cửa sổ Terminal thứ nhất
* **Bước 2**:Trên cửa sổ Terminal thứ hai thực hiện lệnh ping như dưới đây:



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



* **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:



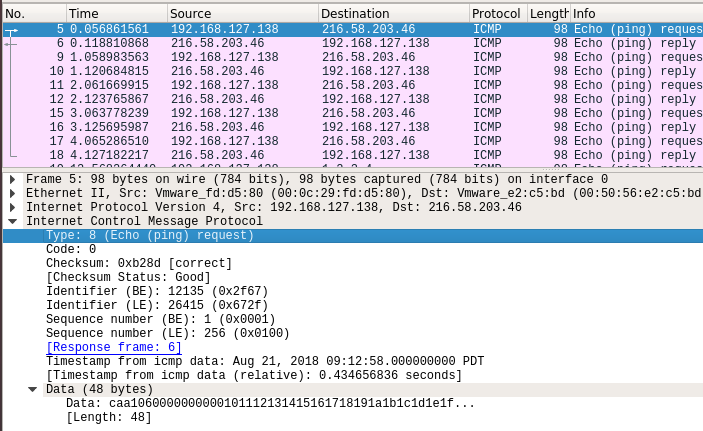
**Phân tích kết quả:**

**-** 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:

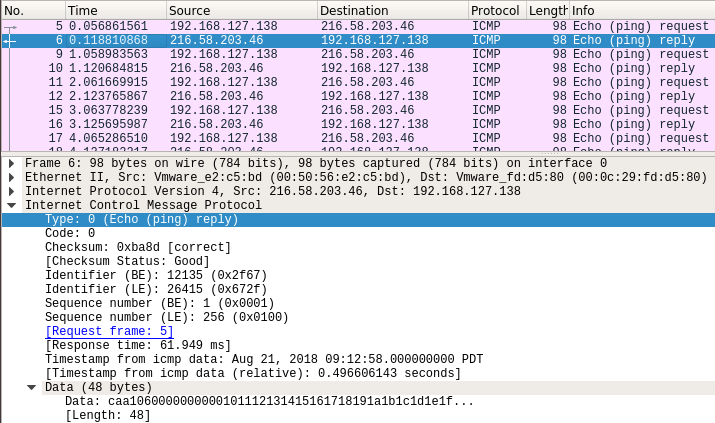
* Địa chỉ IP của máy chủ google.com: 216.58.203.46
* Tên khác của máy chủ: hkg12s10-in-f46.1e100.net
* Kích thước mỗi gói tin: 64 byte
* Số gói gửi: 5; số gói nhận: 5; tỉ lệ mất gói tin (packet loss): 0%
* (Trễ nhỏ nhất/trung bình/lớn nhất/độ lệch)rtt min/avg/max/mdev = 61.747/61.950/62.145/0.202 ms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



- 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 thế thấy nội dung phần Data(48 bytes) giống với gói tin ICMP Eco Request ở trên

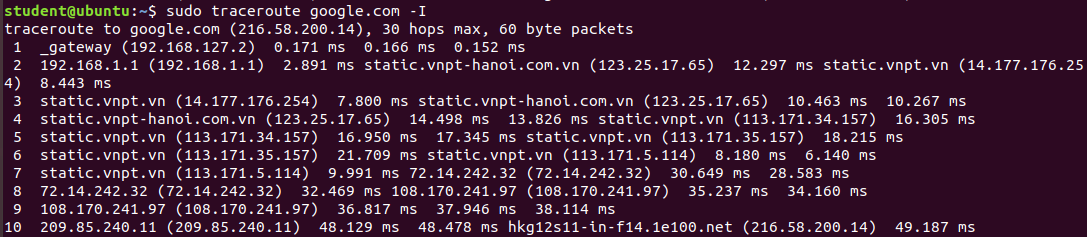


**11.1.2. Sử dụng công cụ traceroute**

*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:*

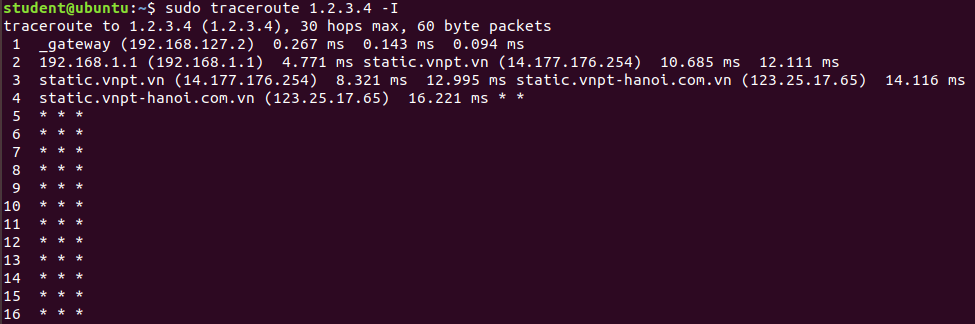
**sudo apt-get install traceroute**

* **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:

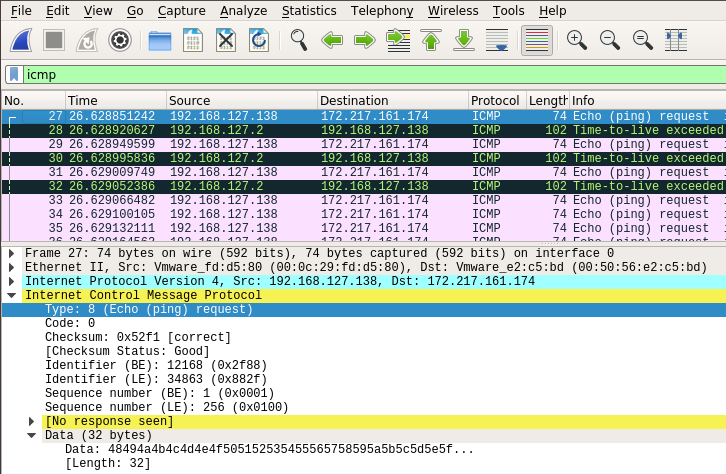


*Lưu ý: Với tùy chọn -I lệnh này sẽ gửi đi các gói tin ICMP Echo Request thay vì dùng các gói tin UDP theo mặc định*

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



* **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:

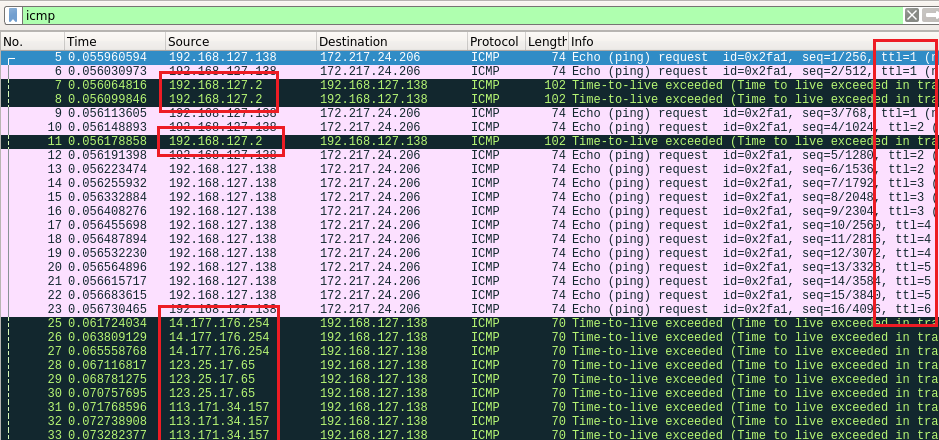


**Phân tích kết quả:**

**-** 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.

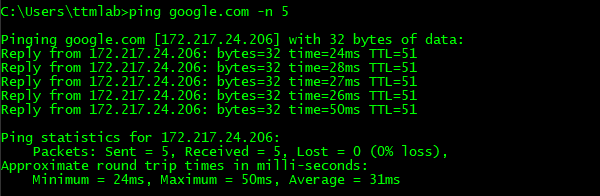


**11.2 Kiểm tra tình trạng kết nối trên Windows**

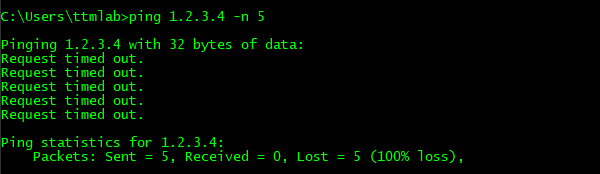
**11.2.1. Sử dụng công cụ ping**

*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.*

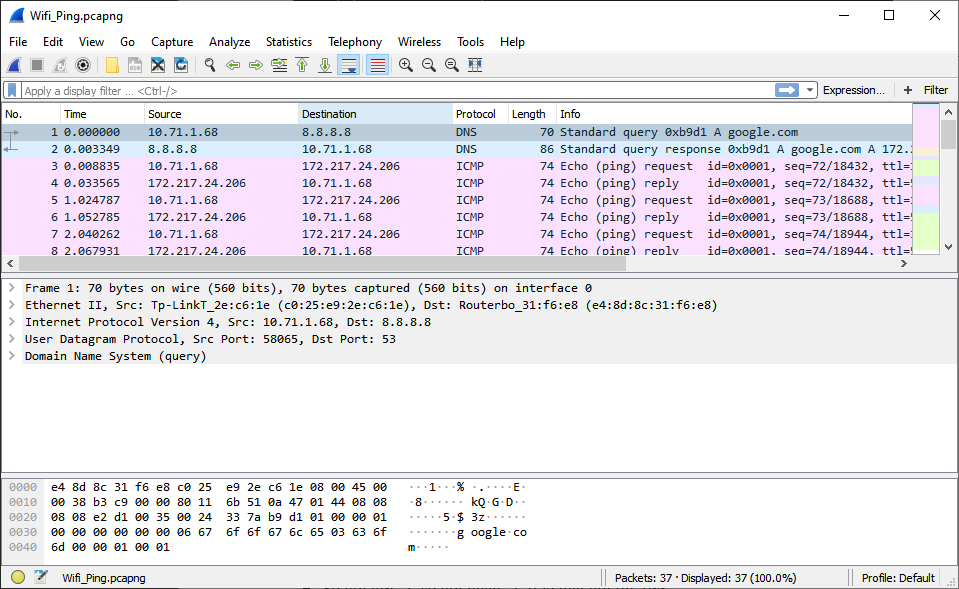
* ***Bước 1***: Mở Windows Explorer vào đường dẫn cài đặt, khởi động Wireshark (ví dụ đường dẫn mặc định là: C:\Program Files\Wireshark\Wireshark.exe).‬‬‬‬‬‬‬‬‬
* ***Bước 2***:Mở Command Prompt thực hiện lệnh ping như dưới đây:



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



* ***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 =

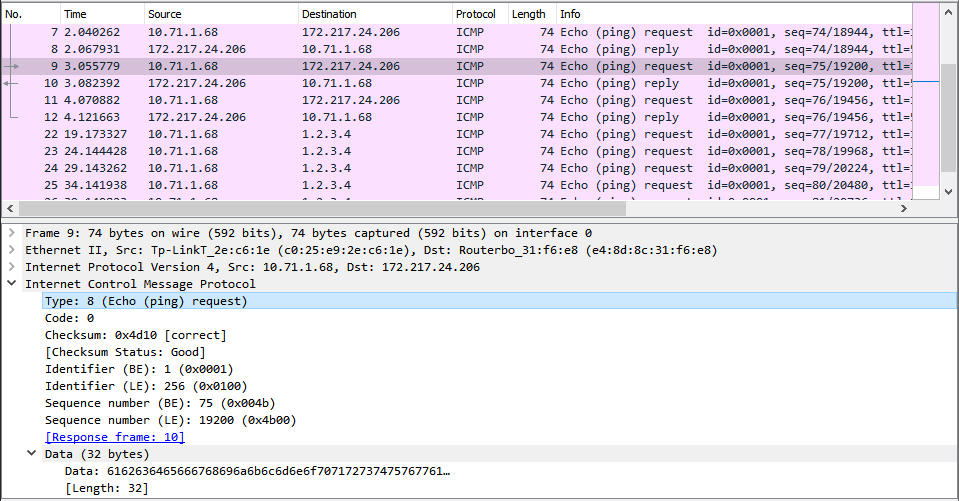
(Approximate round trip times in milli-seconds:

Minimum = 24ms, Maximum = 50ms, Average = 31ms)

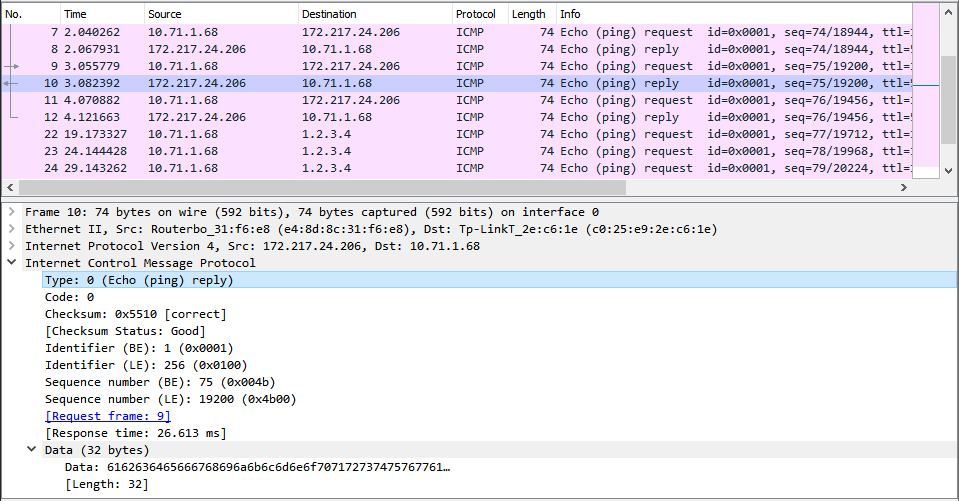
* Thời gian thực hiện lệnh (time): 4008 ms

- 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

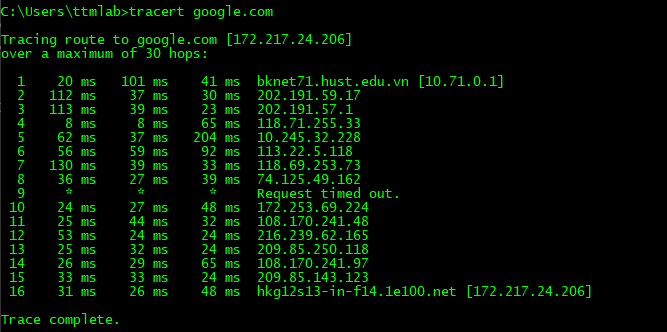


- Mở rộng phần tiêu đề của gói tin Echo (ping) reply của gói trên ta thấy trường Type là 0 cho thấy gói tin này là ICMP Echo Reply. Hơn nữa, ta có thế thấy nội dung phần Data (32 bytes) giống với gói tin ICMP Eco Request ở trên.

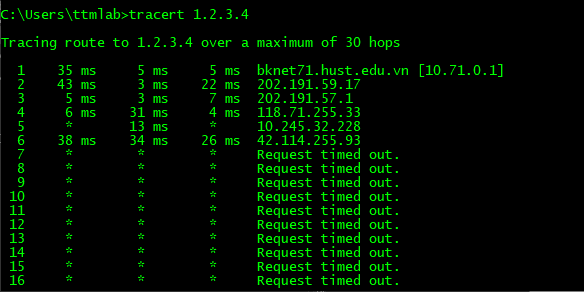


**11.2.2. Sử dụng công cụ tracert**

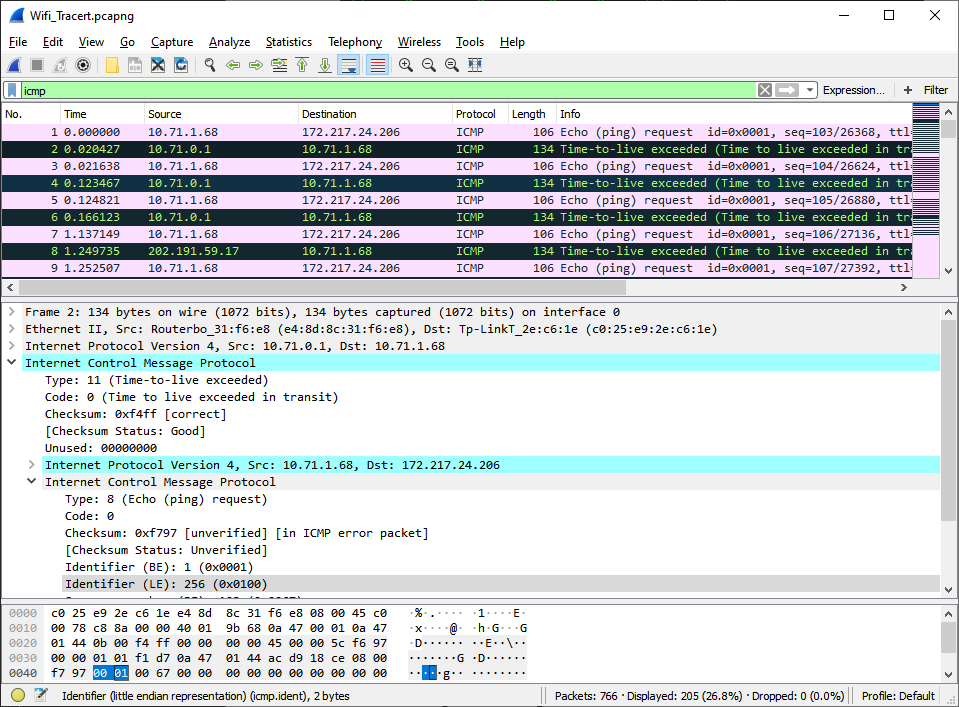
* ***Bước 1***: Mở Windows Explorer vào đường dẫn cài đặt, khởi động Wireshark (ví dụ đường dẫn mặc định là: C:\Program Files\Wireshark\Wireshark.exe).‬‬‬‬‬‬‬‬‬
* ***Bước 2***:Mở Command Prompt thực hiện lệnh tracert như dưới đây:



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



* ***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:

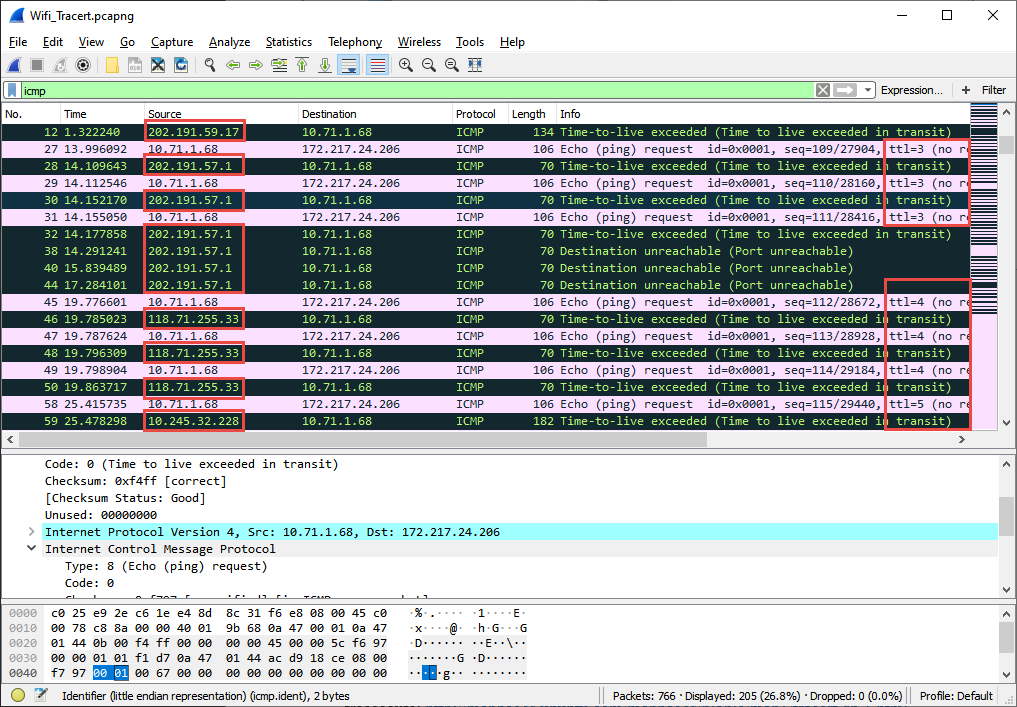


**Phân tích kết quả:**

**-** 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.

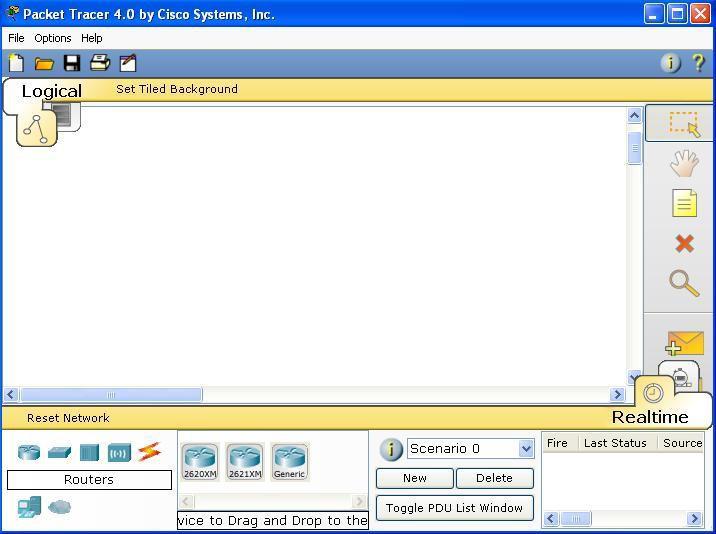
- Trên kết quả bắt gói tin của Wireshark, chúng ta có thể thấy các nhóm 3 gói tin ICMP được gửi đi. Sau khi gửi xong một nhóm, giá trị TTL của nhóm tiếp theo tăng thêm 1. Địa chỉ nguồn của các gói tin báo lỗi ICMP Time to live exceeded chính là địa chỉ các chặng.



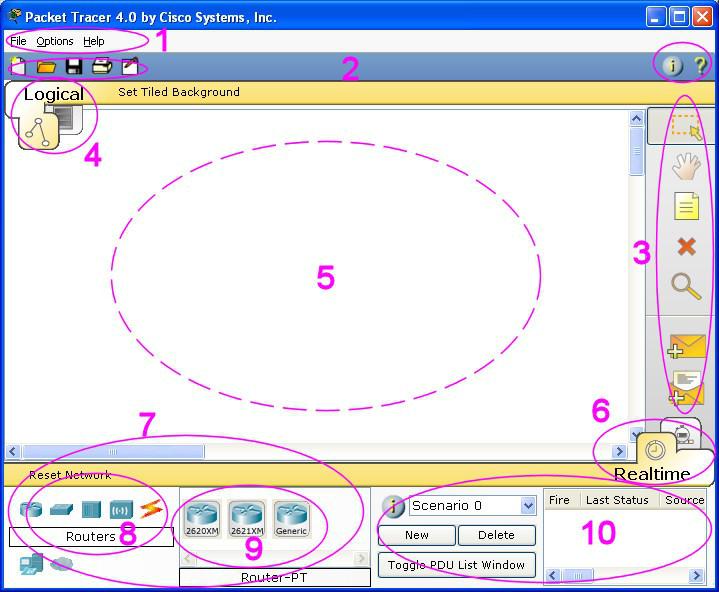
# Phụ lục 5: HƯỚNG DẪN SỬ DỤNG PACKET TRACER

* 1. **Hướng dẫn sử dụng cơ bản**

Giao diện chính của chương trình như sau:



Các khu vực làm việc chính của chương trình:



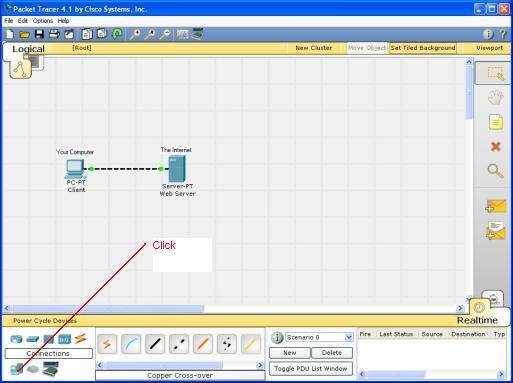
Chi tiết chức năng các MENU:

1. **Menu Bar** : bao gồm các menu **File**, **Options**, **Edit** và **Help** cung cấp các chứcnăng 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 giữaPhysical Workspace và the Logical Workspace
5. **Workspace :** Đây là môi trường để bạn thực hiện thiết kế hệ thống mạng, xem giảlập các thiết bi và các thông tin liên quan…
6. **Realtime/Simulation Bar:** bạn có thể chuyển qua lại giữa **Realtime và**

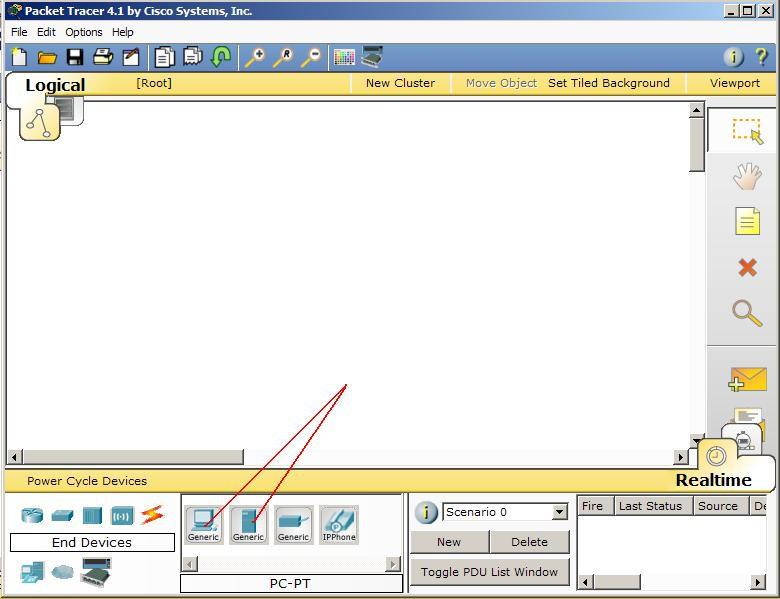
**Simulation mode**

1. **Network Component Box** : Nơi bạn lựa chọn các thiết bị và kết nối giữa chúng…
2. **Device-Type Selection Box :** Gồm những thiết bị được Packet Tracer 4.1 hỗ trợ
3. **Device-Specific Selection Box :** lựa chọn những thiết bị dùng trong hệ thống mạngvà cách thức nối kết giữa chúng
4. **User Created Packet Window\* :** Quản lí các packets mà bạn đặt trong hệ thốngmạng. Xem "Simulation Mode" để nắm rõ hơn về chức năng này
   1. **Hướng dẫn tạo hệ thống đơn giản bao gồm 1 PC và 1 Server kết nối với nhau**

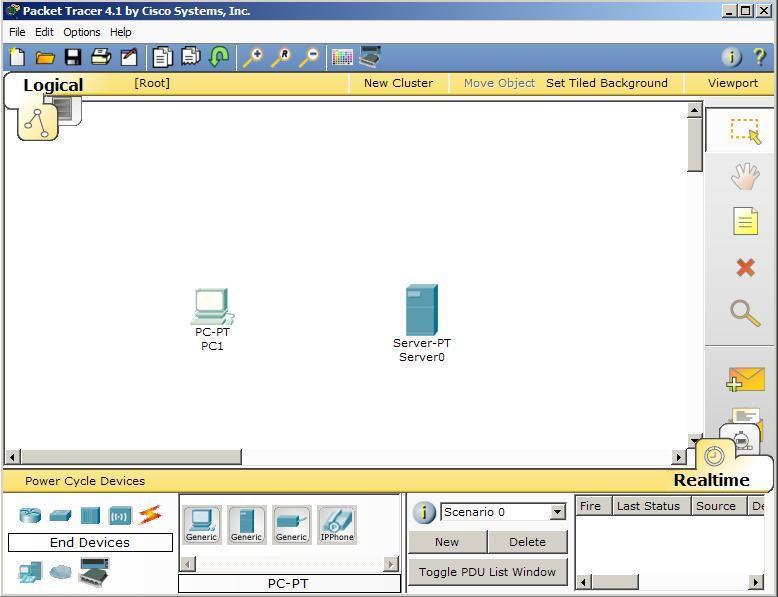
Trong chế độ làm việc **LOGICAL**, bạn lưu ý khư vực số 7, bạn chọn biểu tượng có hình chiếc máy vi tính . **Click** vào đó:



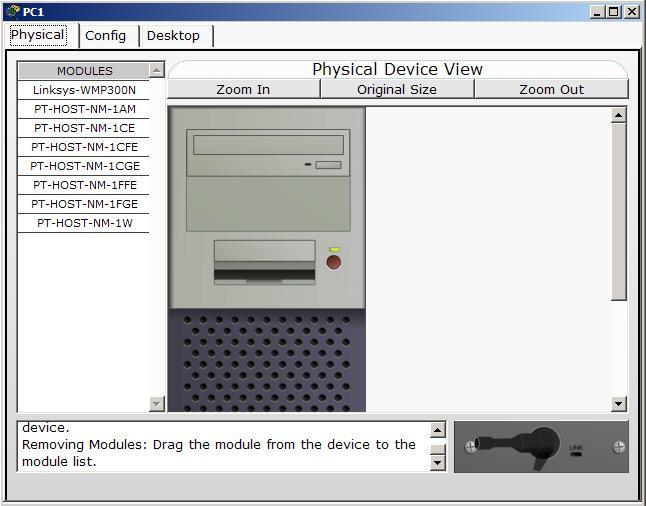
Lần lượt lựa chọn 2 thiết bị cần kết nối là **PC** và **Server**

****

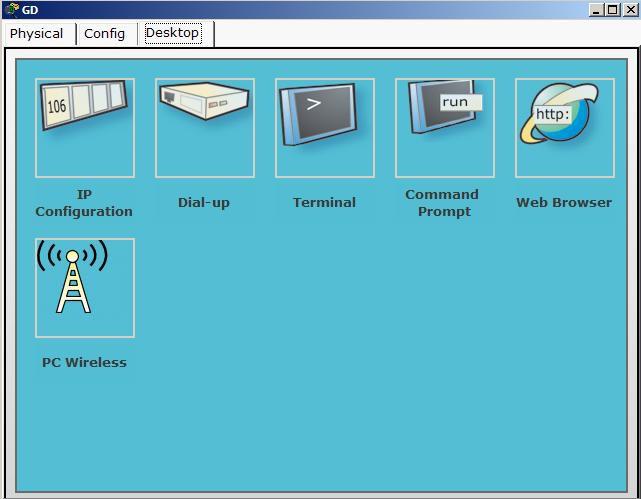
Sau đó lần lượt kéo chúng ra màn hình làm việc như sau:



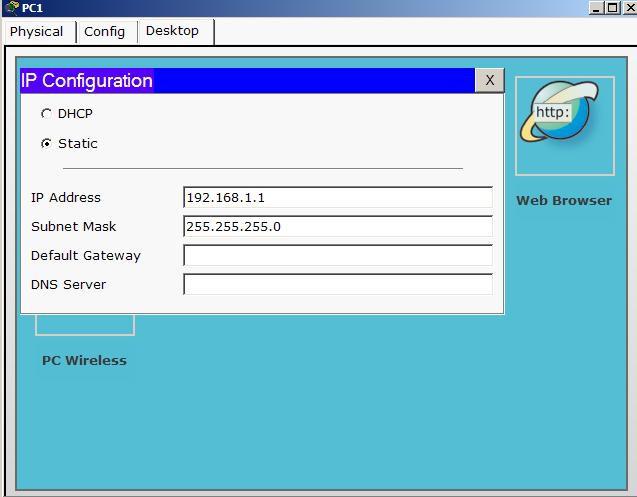
**Click** vào biểu tượng PC trên, chúng ta có thể có thêm những thông tin chi tiết về nó,và có thể tiến hành cài đặt các thông số cho PC đó trên mạng như IP, Gateway, tên máy, loại thiết bị dùng để kết nối vào mạng…



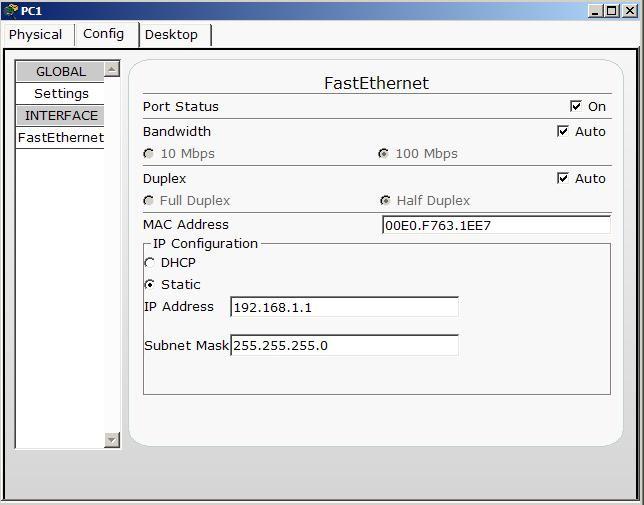
Để cấu hình IP của máy, ta chọn Tab **DESKTOP**:



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

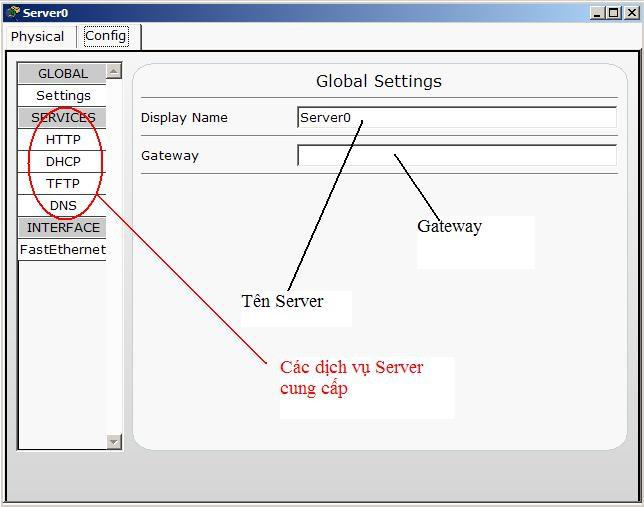


Nếu muốn thay đổi tên máy thì chúng ta chọn **Tab CONFIG**, trong đó sẽ có những lựa chọn cho phép chúng ta xem các thông tin hiện tại của máy tính như: tên máy, địa chỉ Mac, Ip và Gateway hiện thời…

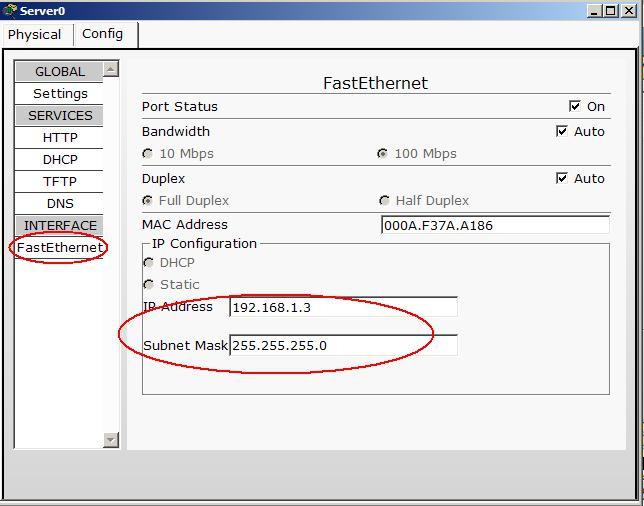


Để tiến hành **cấu hình Server**, chúng ta cũng làm tượng tự, click vào hình Server , 1 bảng các thông tin chi tiết sẽ giúp chúng ta biết và tiến hành cài đặt các thông số cho Server như IP, các dịch vụ HTTP, DNS…

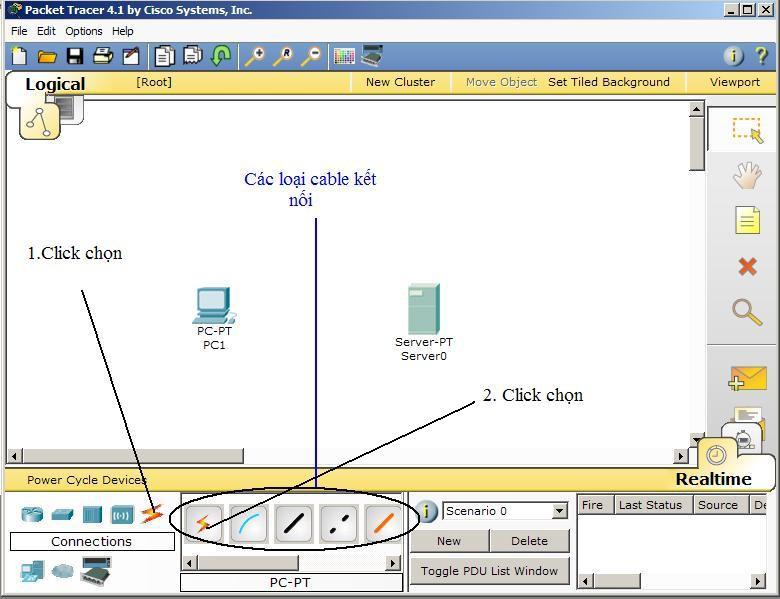
Các thông số cài đặt ở Tab **CONFIG**

****

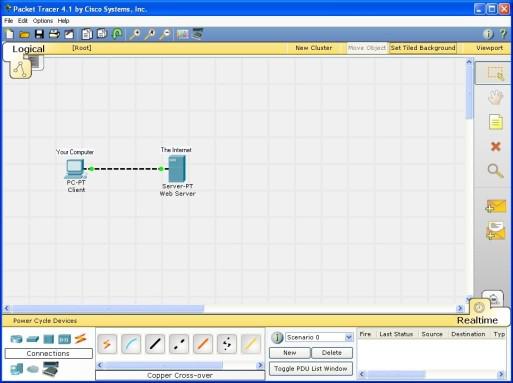
Để cấu hình địa chỉ IP cho Server chúng ta chọn FastEthernet. Sau đó tiến hành cấu hình địa chỉ IP và Subnet Mask cho Server



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

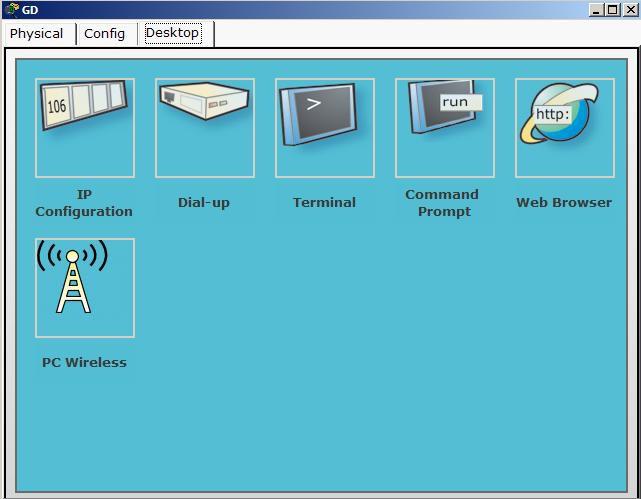


Sau đó chúng ta click vào biểu tượng PC và kết nối với Server như hình sau:

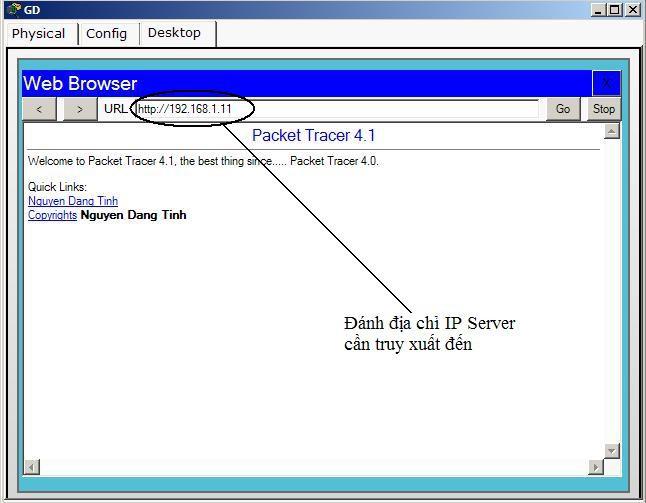


* 1. **Hướng dẫn sử dụng được những dịch vụ mà Server cung cấp**
     1. **Sử dụng dịch vụ HTTP:**

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



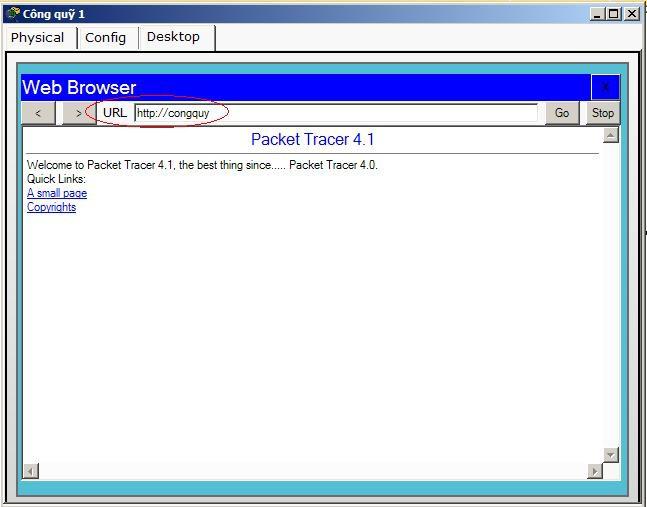
Chọn **Web Browser**, ta sẽ có 1 trình duyệt Web đơn giản giúp chúng ta có thể sử dụng dịch vụ HTTP do Server cung cấp:



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)

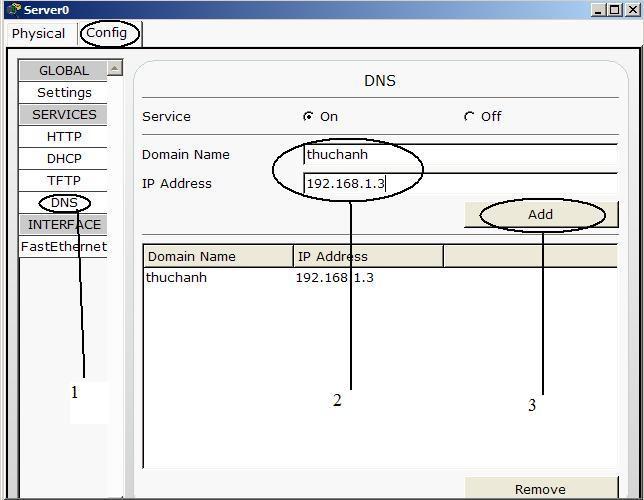
Minh họa như sau:



* + 1. **Hướng dẫn cài đặt dịch vụ DNS cho Server:**

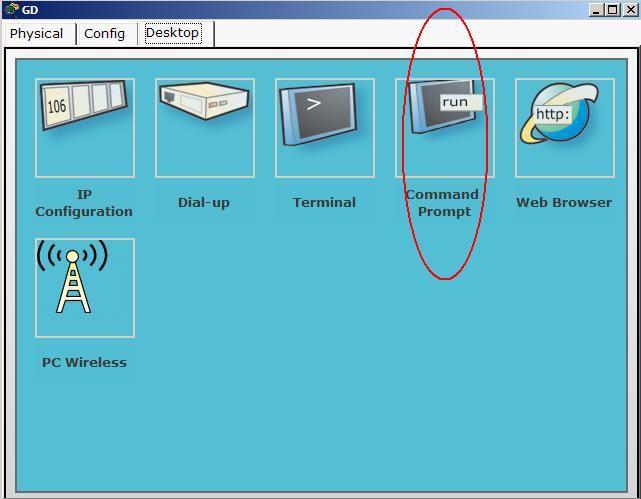
Để cài đặt dịch vụ DNS, chúng ta click đúp vào biểu tượng Server trên màn hình thiết kế.

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

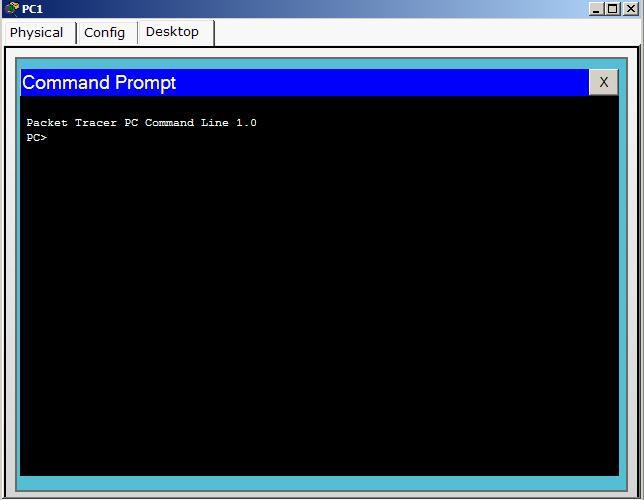


* 1. **Hướng dẫn thực hiện 1 số lệnh cơ bản**

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**

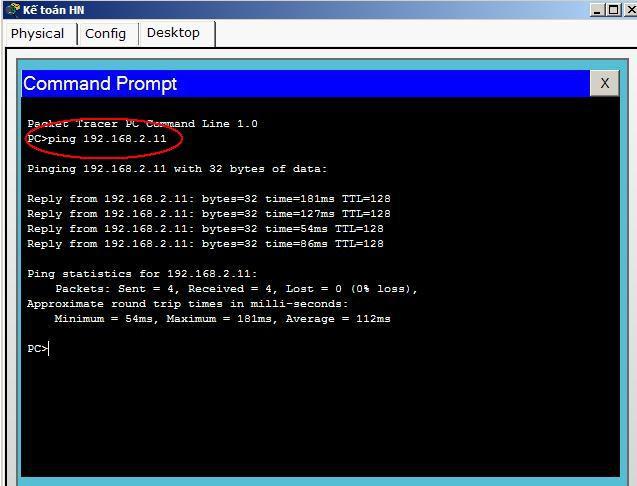
****

Click chọn thì giao diện hiện ra như sau:

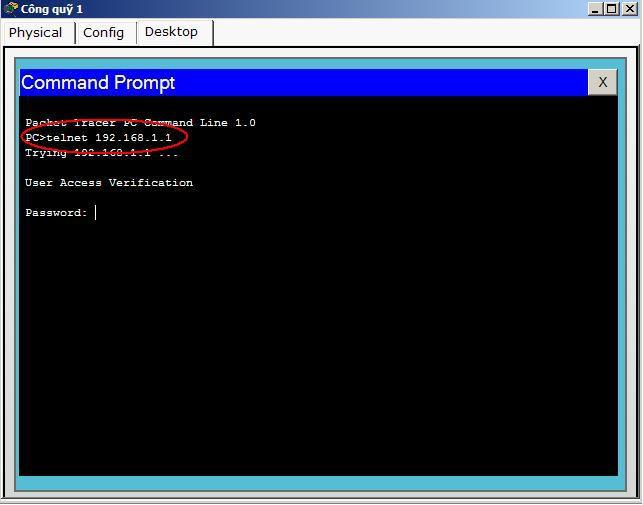


Tại đây chúng ta có thể thực thi các câu lệnh cơ bản mà Packet Tracer hỗ trợ, sau đây là minh họa các câu lệnh cơ bản :

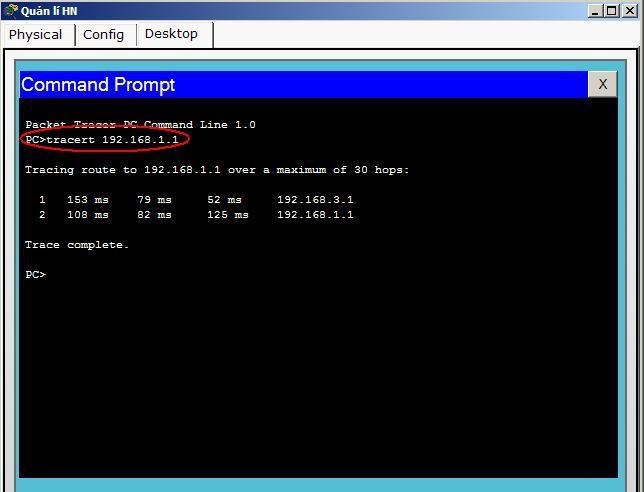
**1.Lệnh PING**



**2.Lệnh TELNET**

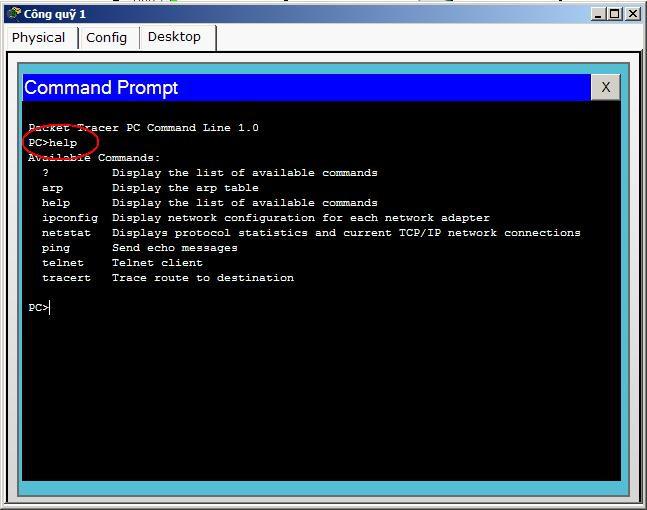


**3.Lệnh TRACERT**



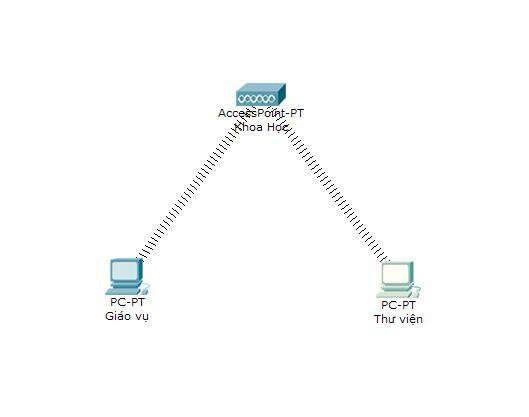
Để muốn biết các thông tin chi tiết về câu lệnh chúng ta có thể đánh lệnh **HELP** hoặc **?**

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



* 1. **HƯỚNG DẪN THIẾT KẾ MẠNG WIRELESS ĐƠN GIẢN TRONG PACKET TRACER**

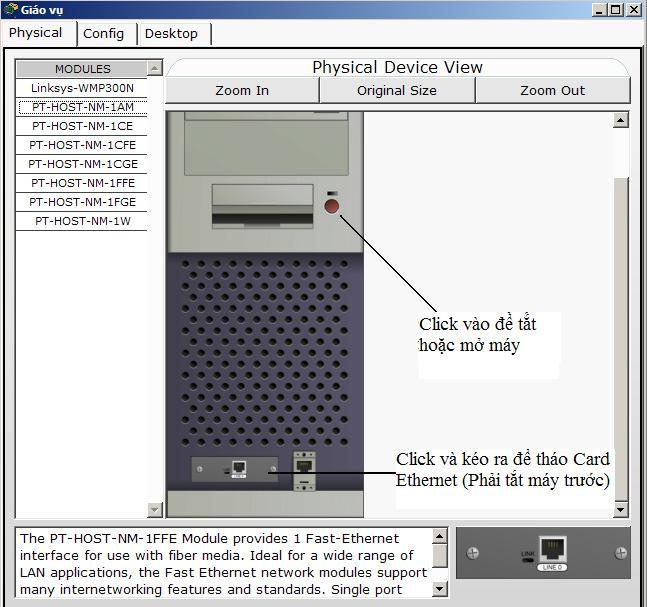
Trong phần này chúng ta sẽ tiến hành thiết kế 1 mạng Wireless đơn giản, minh họa cho mạng như hình sau :



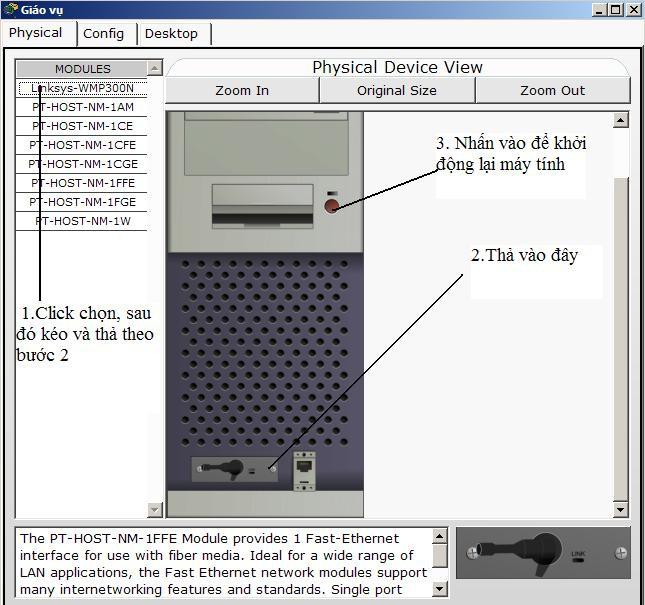
Đối với thiết kế hệ thống mạng , bố trí các thiết bị ta làm tương tự như thiết kế ở trên. Vấn đề chúng ta muốn biết ở đây là làm sao để kết nối thiết bị vào hệ thống mạng Wireless.

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

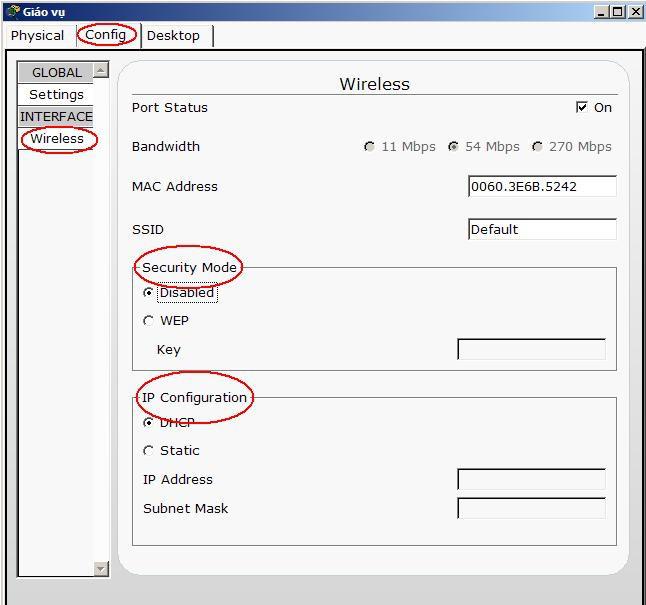
Đầu tiên Click vào biểu tượng PC trong thiết kế của mình, sau đó chọn **Tab Physical,** chúng ta sẽ tắt PC và tháo Card Ethenet, sau đó lắp Card Wireless cho máy. Các bước minh họa như sau:



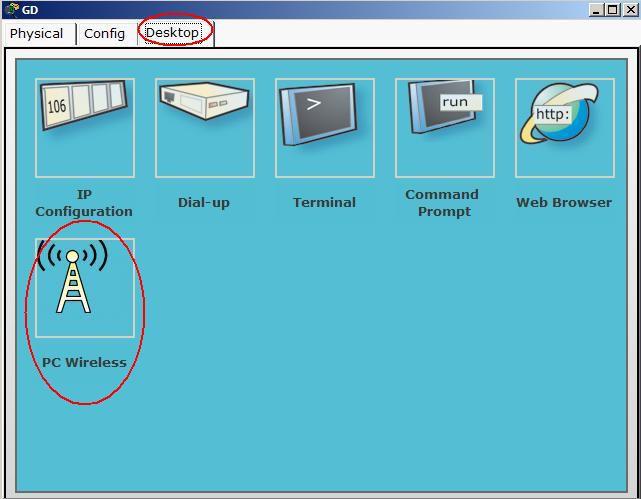
Sau khi đã tháo Card Ethernet ra, chúng ta tiến hành lắp đặt Card Wireless vào máy tính để có thể thu được sóng Wireless. Các bước tiến hành minh họa như hình dưới đây:



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.

