BUỔI THỰC HÀNH 2

Mục đích:

- Sử dụng công cụ tcpdump để bắt các đơn vị dữ liệu gởi nhận qua các giao diện mạng.
- Sử dụng công cụ đồ họa wireshark để hiển thị và phân tích các đơn vị dữ liệu nhận được trực tiếp từ một giao diện mạng hoặc từ một tập tin.
- Giải thích được ý nghĩa của các trường thông tin trong các gói tin của các giao thức phổ biến trên mạng Internet
- Xây dựng mạng ảo kết nối bằng Router và vạch đường tĩnh.

I. GIỚI THIỆU VỀ TCPDUMP

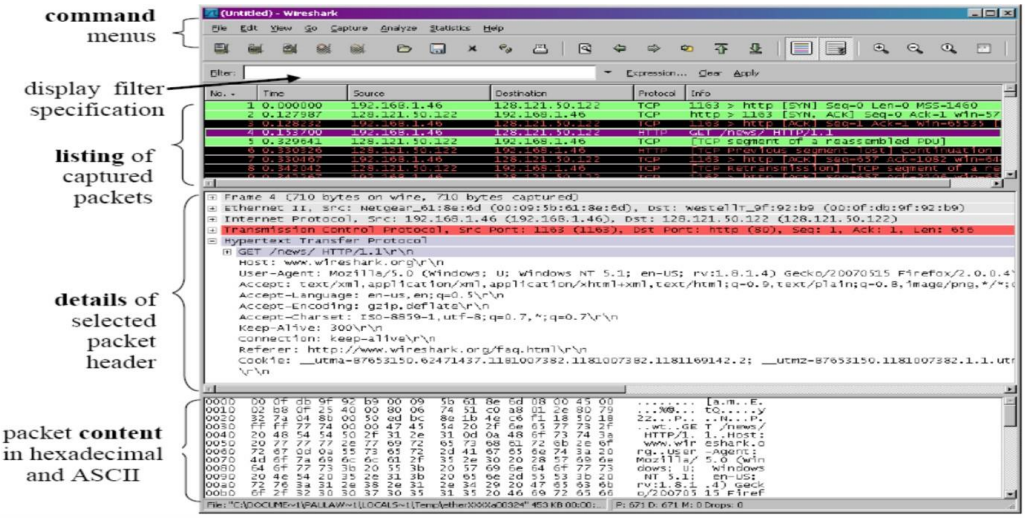
Đọc và thực hiện các bài tập trong các tài liệu sau về tcpdump công cụ để bắt các gói dữ liệu vào ra trên các giao diện mạng của máy tính Linux:

- Tài liệu cơ bản dễ hiểu về tcpdump: https://github.com/hoangdh/tcpdump
- TCPDUMP, những thủ thuật sử dụng?: https://blog.tinohost.com/tcpdump-la-gi/
- Trang tài liệu tiếng anh gốc về tcpdump https://www.tcpdump.org/manpages/tcpdump.1.html

II. GIỚI THIỆU VỀ WIRESHARK

Wireshark là một công cụ mã nguồn mở sử dụng phổ biến trên nhiều hệ điều hành khác nhau. Wireshark cho phép quan sát và phân tích các thành phần trong gói dữ liệu bắt được theo thời gian thực.

Wireshark cung cấp giao diện thân thiện và thuận lợi cho việc phân tích chi tiết các gói dữ liệu.



- ***Thanh menu lệnh***: chứa các lựa chọn để tương tác với file đang được mở.
- ***Bộ lọc*:** lọc và hiển thị dữ liệu tương ứng.
- ***Giao diện liệt kê các gói dữ liệu*:** thể hiện thông tin chi tiết của các gói dữ liệu bắt được như: protocol, source, destination,…
- ***Giao diện thể hiện thông tin của dữ liệu:*** số thứ tự frame, chiều dài frame, khuôn dạng frame, khuôn dạng gói tin IP, giao thức tầng ứng dụng…
- ***Giao diện thể hiện nội dung của dữ liệu bằng mã HEX và mã ASCII***

Sử dụng Wireshark trong phần thực hành Mạng máy tính:

- Wireshark không thể được cài đặt trực tiếp trên máy ảo Kathara do máy ảo Kathara hoạt động dưới chế độ UML (User Mode Linux) không hỗ trợ giao diện đồ họa cho người dùng (GUI).

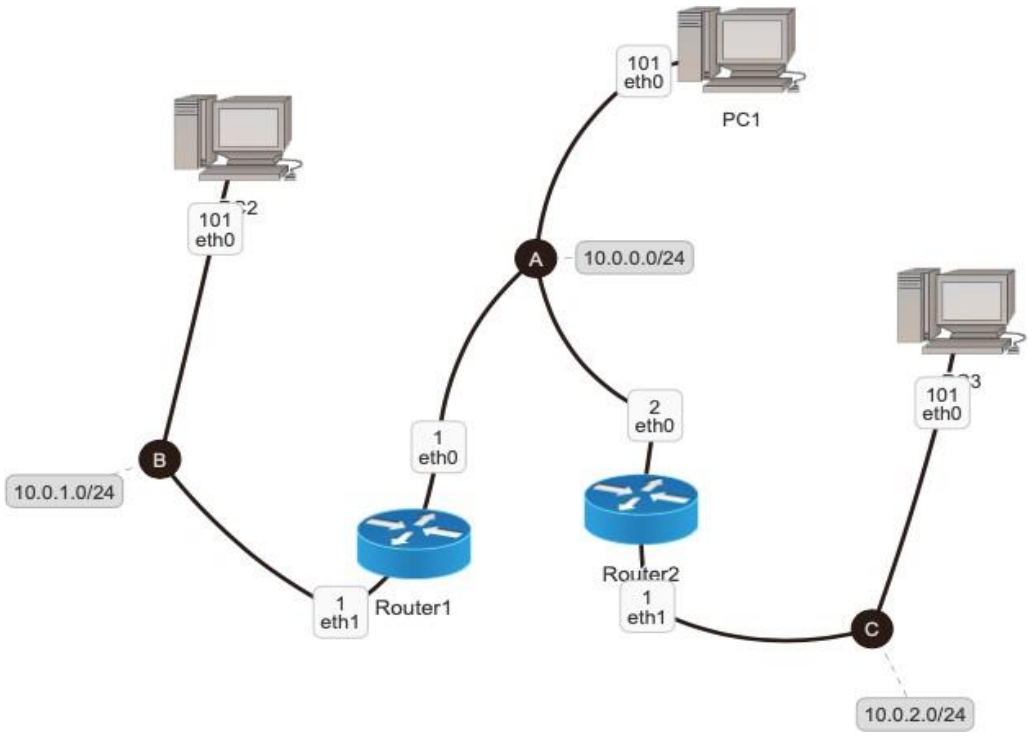
- Trên máy ảo Kathara, công cụ tcpdump được sử dụng thay cho Wireshark để bắt các gói tin (packet sniffer) và ghi nhận dữ liệu bắt được vào trong file có đuôi .pcap. Cách dùng lệnh tcpdump được hướng dẫn cụ thể trong từng bài thực hành.
- Trên máy thực Ubuntu 16.04, các file .pcap sẽ được mở bằng Wireshark. Nhờ vào giao diện đồ họa người dùng (GUI) của Wireshark, sinh viên thực hiện các yêu cầu phân tích gói tin (định dạng, giao thức, địa chỉ...) dễ dàng hơn.

Tài liệu tham khảo

- Sử dụng Wireshark để phân tích gói dữ liệu trong hệ thống mạng
  https://quantrimang.com/su-dung-wireshark-de-phan-tich-goi-du-lieu-trong-he-thong-mang-85026
- Công cụ bảo mật WireShark là gì? Cách sử dụng WireShark ra sao?
  https://vdodata.vn/cong-cu-bao-mat-wireshark/
- Tài liệu tiếng Anh chính thức: https://www.wireshark.org/docs/
  10 Tips On How to Use Wireshark to Analyze Packets in Your Network
  https://www.tecmint.com/wireshark-network-traffic-analyzer-for-linux/

III. BÀI TẬP THỰC HÀNH

BÀI TẬP 5: Mô phỏng mạng ảo như hình phía dưới, cài đặt bảng vạch đường tĩnh và khảo sát giao thức ICMP bằng *Wireshark*



♦ **Bước 1:** Quan sát mô hình mạng cần xây dựng. Nhận diện các thiết bị (PC, Router...), giao diện (eth0, eth1...) với các địa chỉ IP được gán

♦ **Bước 2:** Xây dựng cấu trúc thư mục mạng ảo (nằm dưới thư mục cá nhân */home/student<mã số sinh viên>*) với

đầy đủ các thư mục con và các file cấu hình (***.startup***, ***lab.conf***). Thư mục mạng ảo đặt tên là **BaiTap5**

♦ **Bước 3:** Trên file ***lab.conf***, soạn thảo nội dung mô tả hình thái mạng theo thiết kế

```
pc1[0]=A
pc2[0]=B
pc3[0]=C
router1[0]=A
router1[1]=B
router2[0]=A
router2[1]=C
```

♦ **Bước 4:** Trên file ***PC1.startup***, thông tin vạch đường đến LAN B và C được bổ sung vào bảng vạch đường của PC1 như sau:

```
ifconfig eth0 10.0.0.101/24 up
route add -net 10.0.1.0/24 gw 10.0.0.1
route add -net 10.0.2.0/24 gw 10.0.0.2
```

Ý nghĩa: Lệnh route *add -net <Network Address> gw <Gateway Address>* cho phép thêm thông tin vạch đường (tĩnh) tới 1 mạng trên một thiết bị.

♦ **Bước 5:** Thực hiện tương tự trên ***PC2.startup*** (kết nối đến LAN A và LAN C)

```
ifconfig eth0 10.0.1.101/24 up
route add -net 10.0.0.0/24 gw 10.0.1.1
route add -net 10.0.2.0/24 gw 10.0.1.1
```

và ***PC3.startup*** (kết nối đến LAN A và LAN B)

```
ifconfig eth0 10.0.2.101/24 up
route add -net 10.0.0.0/24 gw 10.0.2.1
route add -net 10.0.1.0/24 gw 10.0.2.1
```

♦ **Bước 6:** Thêm thông tin vạch đường trên ***Router1.startup*** và ***Router2.startup*** bằng lệnh *route add -net* đã được hướng dẫn sao cho Router1 biết đường đi tới LAN C và Router 2 biết đường đi tới LAN B.

Nội dung file ***Router1.startup*** có thể được trình bày như sau:

```
ifconfig eth0 10.0.0.1/24 up
ifconfig eth1 10.0.1.1/24 up
route add -net 10.0.2.0/24 gw 10.0.0.2
```

Thực hiện tương tự cho ***Router2.startup*** của Router2

```
ifconfig eth0 10.0.0.2/24 up
ifconfig eth1 10.0.2.1/24 up
```

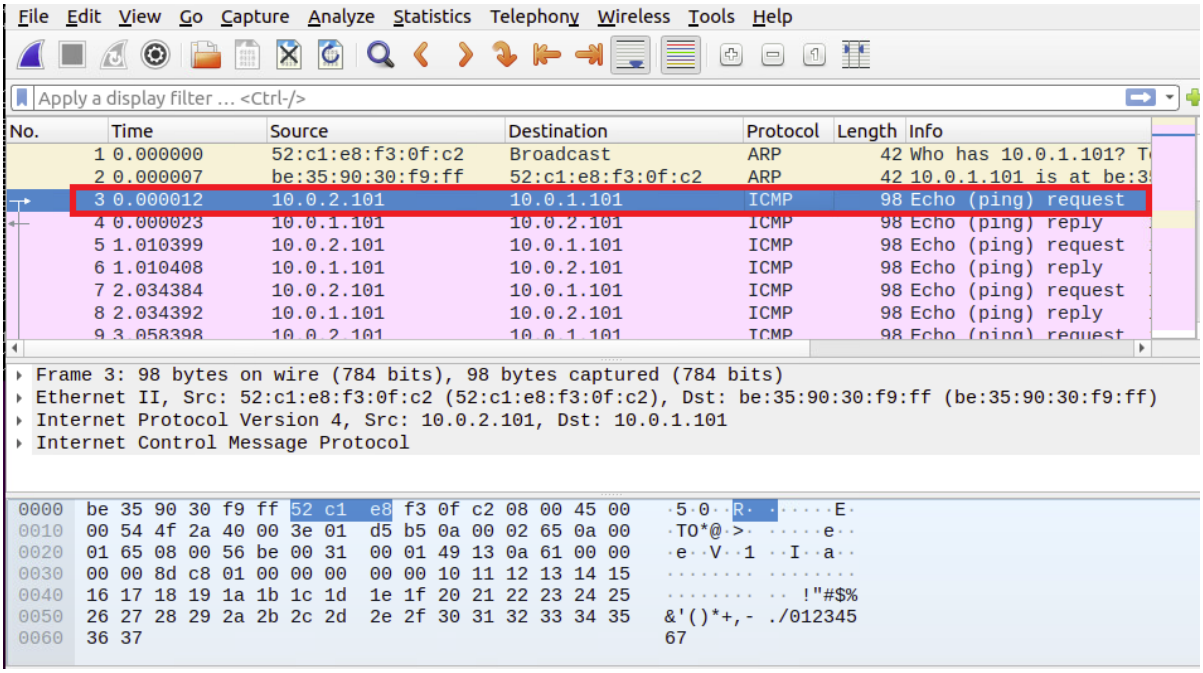
route add -net 10.0.1.0/24 gw 10.0.0.1

- **Bước 7:** Khởi động mạng ảo **BaiTap5 (**bằng lệnh kathara lstart). Kiểm tra các cấu hình IP và các bảng vạch đường *(bằng lệnh **ifconfig** và **route**)* trên từng router và pc. *Lưu ý: Nếu cấu hình IP hoặc/và bảng vạch đường của 1 thiết bị nào đó bị sai, điều chỉnh lại các file cấu hình* (***.startup***, ***lab.conf***) và *khởi động lại mạng ảo (bằng lệnh* kathara lrestart*).*
- **Bước 8:** Trên PC2, Router1 và Router2 lần lượt thực hiện lệnh ***tcpdump*** với cú pháp như sau:

```
tcpdump -s 1536 -w /shared/BT5_PC2.pcap (trên máy ảo PC2)
tcpdump -s 1536 -w /shared/BT5_Router1.pcap (trên máy ảo Router1)
tcpdump -s 1536 -w /shared/BT5_Router2.pcap (trên máy ảo Router2)
```

Ý nghĩa: Thông tin về các gói tin bắt được (sniffed) sẽ được lưu vào file .pcap trong thư mục ***/shared*** dùng để chia sẻ các tài nguyên giữa máy thực Ubuntu và máy ảo Kathara (PC1, PC2...)

- **Bước 9:** Trên PC3 thực hiện lệnh ***ping*** đến PC2 (ping 10.0.1.101) và chờ khoảng 10 giây. Sau đó dừng lệnh ***ping*** trên PC3 và các các lệnh ***tcpdump*** trên PC2, Router1 và Router2 (*gõ tổ hợp phím Ctrl C)*
- **Bước 10:** Trên máy thực Ubuntu, dùng Wireshark mở các file ***BT5_PC2.pcap (nằm trong thư mục BaiTap5/shared)***, chọn khung vật lý (frame) số 3 *(là khung ICMP đầu tiên, như hình bên dưới)*



Câu hỏi 1:

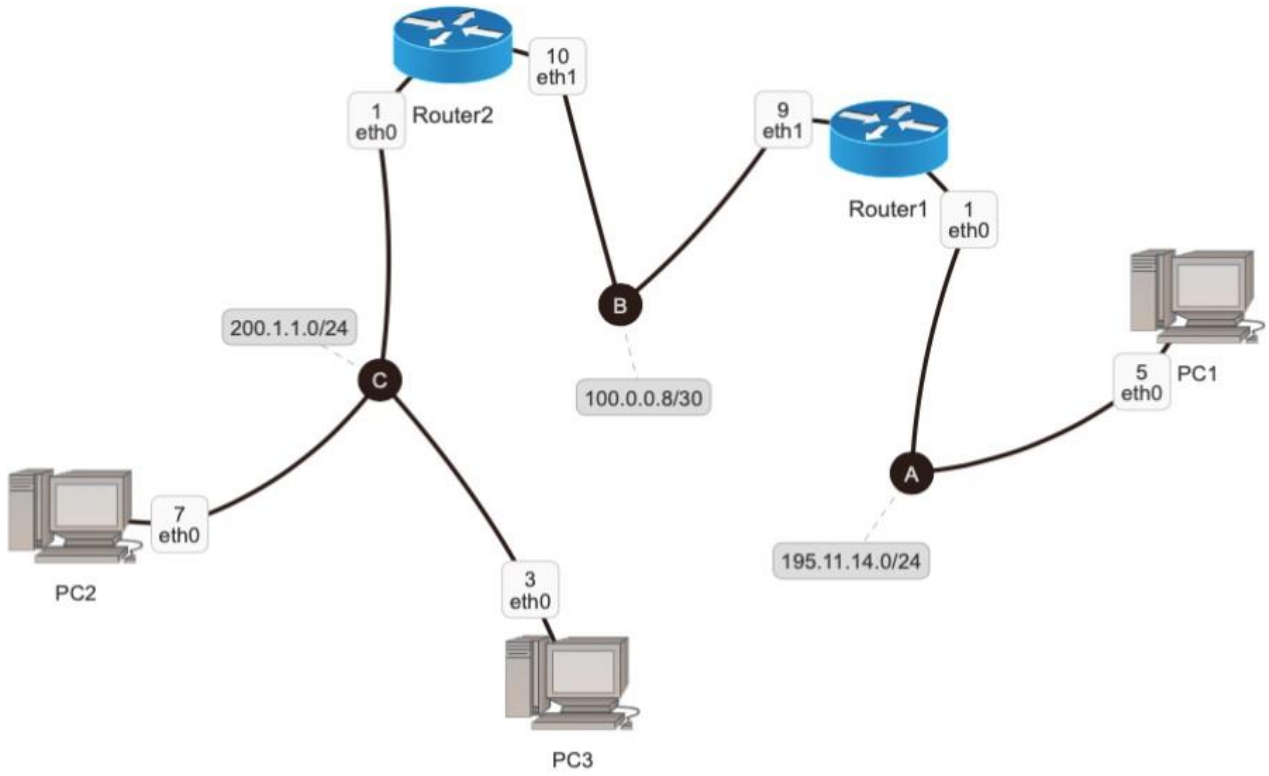
- Toàn bộ khung số 3 có kích thước là bao nhiêu (Bytes)?
- Chọn ***Header Internet Control Message Protocol*** trong khung và cho biết:
  - Gói tin này sử dụng giao thức gì? Giao thức này hoạt động trên tầng nào của mô hình OSI?
  - Thông điệp của giao thức này là gì? Thông điệp này có độ dài bao nhiêu (bytes)?
- Chọn ***Header Internet Protocol Version 4*** và cho biết:
  - Địa chỉ IP của máy gửi dữ liệu là bao nhiêu? Địa chỉ IP này là của máy tính nào trong mạng?
  - Địa chỉ IP của máy nhận dữ liệu là bao nhiêu? Địa chỉ IP này là của máy tính nào trong mạng?
  - Định danh (ID) của gói tin IP này là bao nhiêu (dạng Hexadecimal). Định danh của 1 gói tin có ý nghĩa gì trong thông điệp IP?
  - Độ dài phần Header của thông điệp IP là bao nhiêu? Phần Header bao gồm những trường nào? Mỗi trường có độ dài bao nhiêu (Bytes)
  - Trường Total Length có độ dài là bao nhiêu (Bytes). Hãy lý giải tại sao có độ dài như vậy?
- Chọn ***Header Ethernet II*** và cho biết:
  - Địa chỉ MAC của máy gửi dữ liệu là bao nhiêu? Có phải là địa chỉ MAC của máy tính có địa

chỉ IP (source) đã tìm được trong câu trên không? Nếu không, hãy lý giải và cho biết địa chỉ MAC này là của máy tính nào trong mạng?

- Địa chỉ MAC của máy nhận dữ liệu là bao nhiêu? Có phải là địa chỉ MAC của máy tính có địa chỉ IP (destination) đã tìm được trong câu trên không? Nếu không, hãy lý giải và cho biết địa chỉ MAC này là của máy tính nào trong mạng?
- Trường Type mang giá trị (Hexadecimal) bằng bao nhiêu? Thông tin thể hiện là gì?
- Hãy chỉ ra trường Payload của khung Ethernet II? Trường Payload này có độ dài bằng bao nhiêu (Bytes)?

♦ **Bước 11:** Hủy mạng ảo bằng lệnh kathara lclean sau khi đã thực hiện xong

Bài tập 5 BÀI TẬP 6: Vạch đường tĩnh và gói tin ARP



♦ **Bước 1:** Quan sát mô hình mạng cần xây dựng. Nhận diện các thiết bị (PC, Router...), giao diện (eth0, eth1...) với các địa chỉ IP được gán

♦ **Bước 2:** Xây dựng cấu trúc thư mục mạng ảo (nằm dưới thư mục cá nhân */home/student<mã số sinh viên>*) với đầy đủ các thư mục con và các file cấu hình (***.startup***, ***lab.conf***). Thư mục mạng ảo đặt tên là **BaiTap6**

♦ **Bước 3:** Trên file ***lab.conf***, soạn thảo nội dung mô tả hình thái mạng theo thiết kế

♦ **Bước 4:** Trên file ***PC1.startup***, ***PC2.startup*** và ***PC3.startup***, thông tin vạch đường được bổ sung vào bảng vạch đường bằng lệnh ***route add default gw*** hoặc lệnh ***route add -net*** đã giới thiệu

♦ **Bước 5:** Trên file ***Router1.startup*** và ***Router2.startup*** cũng thực hiện bổ sung thông tin vạch đường vào bảng vạch đường sao cho Router1 biết đường đi tới LAN C và Router 2 biết đường đi tới LAN A.

♦ **Bước 6:** Khởi động mạng ảo **BaiTap6 (**bằng lênh kathara lstart). Kiểm tra các cấu hình IP và các bảng vạch đường *(bằng lệnh **ifconfig** và **route**)* trên từng router và pc.

Lưu ý: Nếu cấu hình IP hoặc/và bảng vạch đường của 1 thiết bị nào đó bị sai, điều chỉnh lại các file cấu hình (***.startup***, ***lab.conf***) và k*hởi động lại mạng ảo (bằng lệnh* kathara lrestart*).*

A – Giao thức ARP giữa 2 thiết bị trong cùng mạng LAN

♦ **Bước 7A:** Trường hợp bảng vạch đường của các thiết bị đều đúng, trên máy ảo PC3, PC2 và Router2, lần lượt thực hiện lệnh ***arp*****,**

Câu hỏi 2: Kết quả hiện thị là gì? nhận xét?

♦ **Bước 8A:** Trên PC2, Router1 và Router2 lần lượt thực hiện lệnh ***tcpdump*** với cú pháp như sau:

tcpdump -s 1536 -w /shared/BT6_PC2.pcap (trên máy ảo PC2)

tcpdump -s 1536 -w /shared/BT6_Router1.pcap (trên máy ảo Router1)

tcpdump -s 1536 -w /shared/BT6_Router2.pcap (trên máy ảo Router2)

♦ **Bước 9A:** Trên PC3 thực hiện lệnh ***ping*** đến PC2 (ping 200.1.1.7) và chờ khoảng 10 giây, sau đó dừng lệnh ***ping*** trên PC3 và các lệnh ***tcpdump*** trên PC2, Router1 và Router2 lại.

♦ **Bước 10A:** Trên PC3 thực hiện lại lệnh ***arp***

Câu hỏi 3: kết quả hiển thị là gì?nhận xét kết quả hiển thị? Có sự thay đổi so với kết quả ở bước số 7A hay không? Lý giải cho sự thay đổi này?

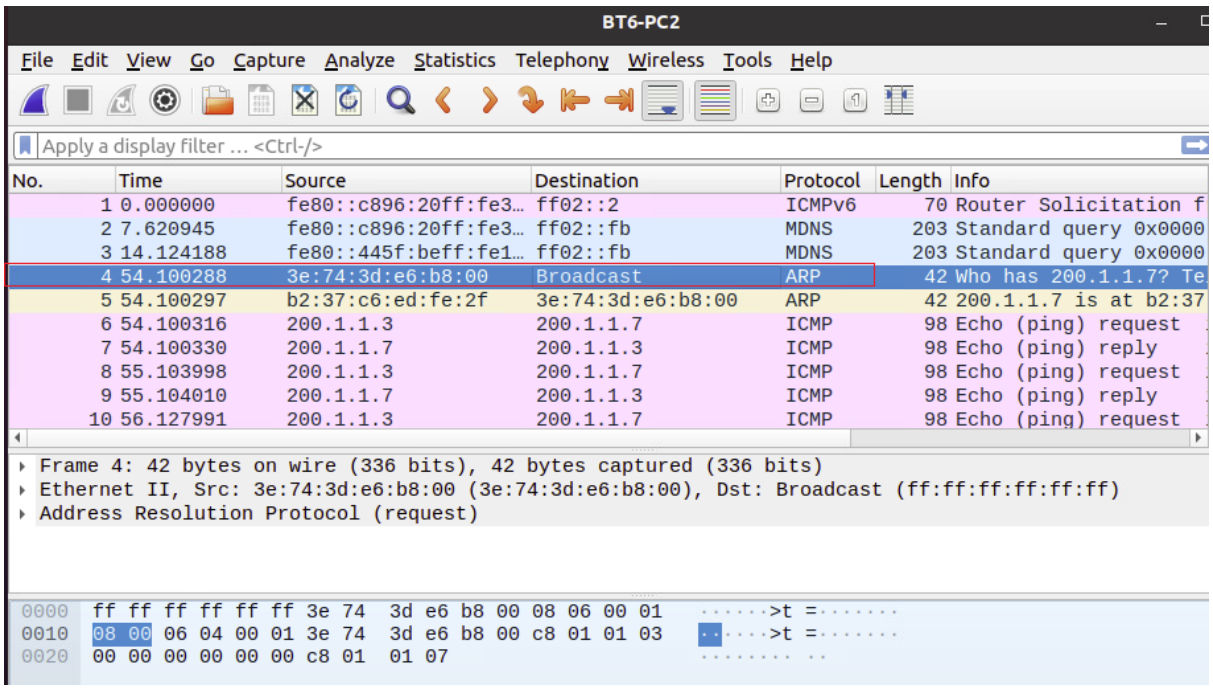
♦ **Bước 11A:** Trên PC2, thực hiện lại lệnh ***arp***

Câu hỏi 4: kết quả hiển thị là gì?nhận xét kết quả hiển thị? Có sự thay đổi so với kết quả ở bước số 7A hay không? Lý giải cho sự thay đổi này?

♦ **Bước 12A:** Trên Router2, thực hiện lại lệnh ***arp***

Câu hỏi 5: kết quả hiển thị là gì? nhận xét kết quả hiển thị? Có sự thay đổi so với kết quả ở bước số 7A hay không? Lý giải cho sự thay đổi này?

♦ **Bước 13A:** Trên máy thực Ubuntu, dùng Wireshark mở các file ***BT6_Router2.pcap (nằm trong thư mục BaiTap5/shared)***, chọn khung vật lý (frame) số 4 *(là khung ARP đầu tiên, như hình bên dưới)*



Câu hỏi 6:

- Toàn bộ khung có kích thước là bao nhiêu (Bytes)?
- Chọn ***Header Address Resolution Protocol*** và cho biết :
  - Trường Opcode có giá trị (Hexadecimal) là bao nhiêu? Giá trị của trường này thể hiện thông tin gì? Trường Opcode này còn có thể có giá trị (Hexadecimal) là bao nhiêu nữa và giá trị đó thể hiện thông tin gì?
  - Địa chỉ IP và địa chỉ MAC của máy gửi dữ liệu? Đây là địa chỉ IP và MAC của máy tính nào trong mạng?
  - Địa chỉ IP và địa chỉ MAC của máy nhận dữ liệu? Đây là địa chỉ IP và MAC của máy tính nào trong mạng? Nhận xét về cặp địa chỉ IP và MAC của máy nhận dữ liệu
- Chọn ***Header Ethernet II*** và cho biết:
  - Địa chỉ MAC của máy gửi dữ liệu là bao nhiêu? Địa chỉ MAC này là của máy tính nào trong mạng?
  - Địa chỉ MAC của máy nhận dữ liệu là bao nhiêu? Địa chỉ MAC này là của máy tính nào

trong mạng? Nhận xét về địa chỉ MAC này và địa chỉ MAC của máy nhận dữ liệu đã quan sát được ở phần ***Header Address Resolution Protocol***

- Trường Type mang giá trị (Hexadecimal) bằng bao nhiêu? Thông tin thể hiện là gì?

B – Giao thức ARP giữa 2 thiết bị khác mạng LAN

♦ **Bước 7B:** Trên máy ảo PC1 và Router1, lần lượt dùng lệnh ***arp***

Câu hỏi 7: Kết quả hiện thị là gì? nhận xét?

♦ **Bước 8B:** Trên PC1, Router1 và Router2 lần lượt thực hiện lệnh ***tcpdump*** với cú pháp như sau:

tcpdump -s 1536 -w /shared/BT6_PC1.pcap (trên máy ảo PC2)
tcpdump -s 1536 -w /shared/BT6_Router1.pcap (trên máy ảo Router1)
tcpdump -s 1536 -w /shared/BT6_Router2.pcap (trên máy ảo Router2)

♦ **Bước 9B:** Trên PC3 thực hiện lệnh ***ping*** đến PC1 (195.11.14.5) và chờ khoảng 10 giây sau đó dừng lệnh ***ping*** trên PC3 và các lệnh ***tcpdump*** trên PC1, Router1 và Router2 lại.

♦ **Bước 10B:** Trên PC3 thực hiện lại lệnh ***arp*** và

Câu hỏi 8: nhận xét kết quả hiển thị? so sánh với bước số 10A?

♦ **Bước 11B:** Trên Router2, thực hiện lại lệnh ***arp***

Câu 9: nhận xét kết quả hiển thị? so sánh với bước số 12A?

♦ **Bước 12B:** Trên Router1, thực hiện lại lệnh ***arp***

Cấu 10: nhận xét kết quả hiển thị?

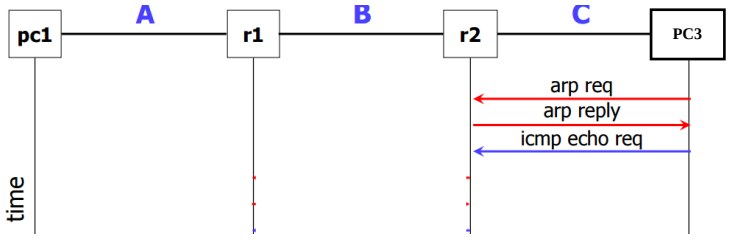
♦ **Bước 13B:** Trên PC1, thực hiện lại lệnh ***arp***

Câu hỏi 11: Nhận xét kết quả hiển thị? so sánh với bước số 7B.

♦ **Bước 14B:** Trên máy thực Ubuntu 16.04, dùng Wireshark mở các file ***BT6_Router1.pcap***, chọn khung vật lý (frame) số 4 *(là khung ARP đầu tiên)*

Câu hỏi 12: Trả lời lại các câu hỏi giống như phần 13A (Câu hỏi 6)

Vẽ sơ đồ tuần tự thể hiện vai trò của giao thức ARP và ICMP trong việc truyền tải dữ liệu từ PC3 đến PC1 bằng lệnh ***ping***



♦ **Bước 15:** Trên PC1, ***ping*** đến địa chỉ 8.8.8.8 (địa chỉ ngoài mạng ảo). Kiểm tra sự hoạt động của giao thức ARP và kết quả hiển thị trên khi dùng lệnh ***arp*** trên PC1 và Router1

♦ **Bước 16:** Trên PC1, ***ping*** đến địa chỉ 195.11.14.200 (địa chỉ thuộc mạng ảo A nhưng không được gán cho máy tính nào cả). Kiểm tra sự hoạt động của giao thức ARP và kết quả hiển thị trên khi dùng lệnh ***arp*** trên PC1 và Router1

♦ **Bước 17:** Hủy mạng ảo bằng lệnh **kathara lclean** sau khi đã thực hiện xong **Bài tập 6**

Bài tập 7: Vạch đường tĩnh trên mạng phức tạp

♦ **Bước 1:** Quan sát mô hình mạng cần xây dựng. Nhận diện các thiết bị (PC, Router...), giao diện (eth0, eth1...) với các địa chỉ IP được gán

♦ **Bước 2:** Xây dựng cấu trúc thư mục mạng ảo (nằm dưới *workspace /home/your_workspace*) với đầy đủ các thư mục con và các file cấu hình (***.startup***, ***lab.conf***). Thư mục mạng ảo đặt tên là **BaiTap7**

♦ **Bước 3:** Trên file ***lab.conf***, soạn thảo nội dung mô tả hình thái mạng theo thiết kế

♦ **Bước 4:** Trên file ***PC1.startup***, ***PC2.startup*** và ***PC3.startup***, thông tin vạch đường được bổ sung vào bảng vạch đường bằng lệnh ***route add default gw*** hoặc lệnh ***route add -net*** đã giới thiệu

♦ **Bước 5:** Trên file ***Router1.startup***, ***Router2.startup*** và ***Router3.startup*** cũng thực hiện bổ sung thông tin vạch đường vào bảng vạch đường sao cho các Router đều có thể vạch đường tới tất cả các mạng LAN

Câu hỏi 13: nội dung tất cả các file .conf và .startup là gì?

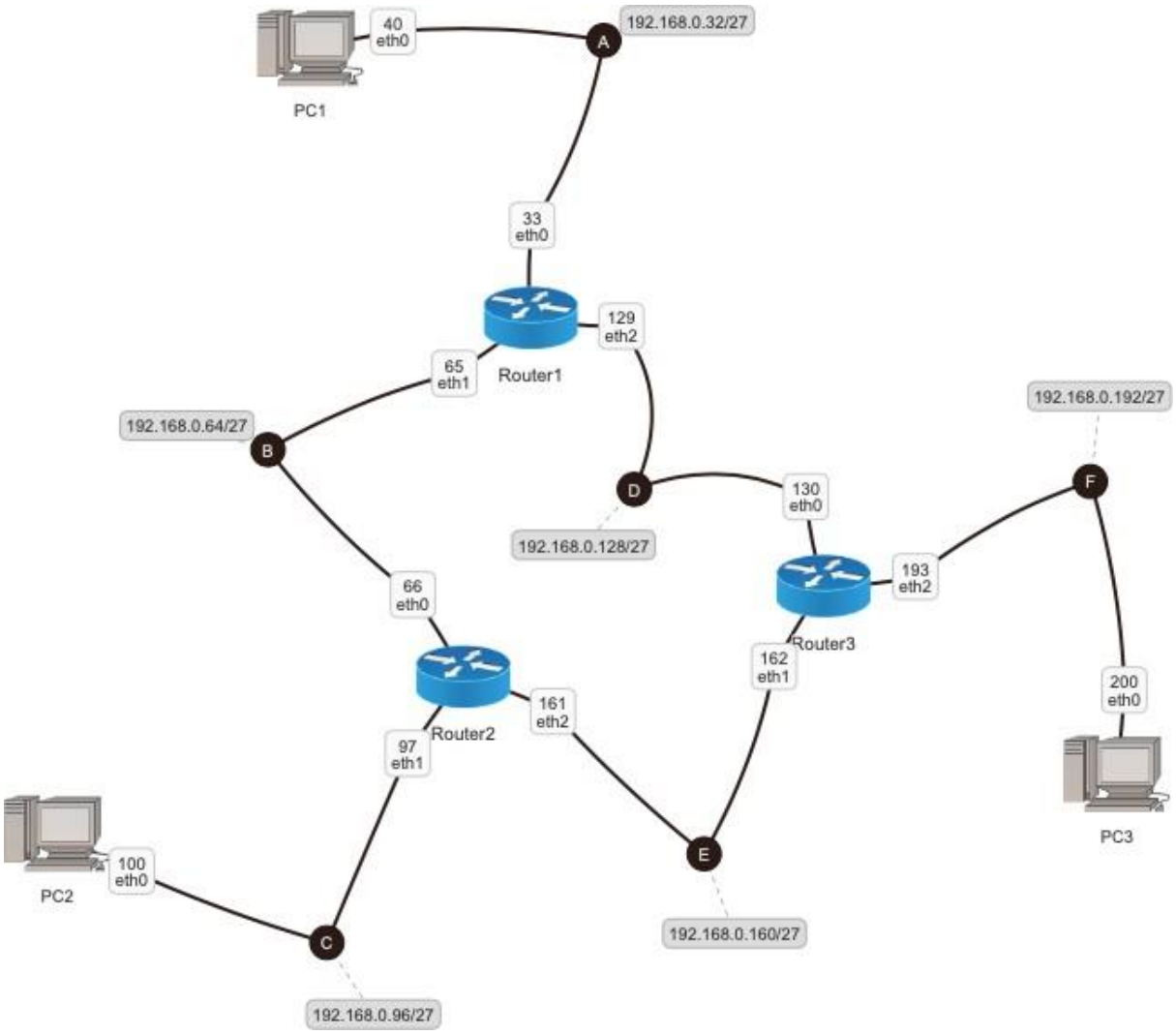
♦ **Bước 6:** Khởi động mạng ảo **BaiTap7**. Kiểm tra bảng vạch đường (bằng lệnh ***route***) trên từng thiết bị mạng.

Câu hỏi 14: Bảng vạch đường của mỗi thiết bị có bao nhiêu đường đi? liệt kê các đường đi này? Kiểm tra với mô hình xem đúng không?

♦ **Bước 7:** Kiểm tra tính liên thông giữa các máy tính PC1, PC2 và PC3 trong mạng (bằng lệnh ***ping***)

Câu hỏi 15: kết quả hiển thị là gì?

♦ **Bước 8:** Hủy mạng ảo bằng lệnh **kathara lclean** sau khi đã thực hiện xong **Bài tập 7**


40
eth0
192.168.0.32/27
A
PC1
33
eth0
129
eth2
65
eth1
Router1
192.168.0.64/27
B
D
130
eth0
192.168.0.128/27
192.168.0.192/27
F
193
eth2
Router3
66
eth0
162
eth1
Router2
161
eth2
97
eth1
200
eth0
PC3
PC2
100
eth0
E
C
192.168.0.160/27
192.168.0.96/27