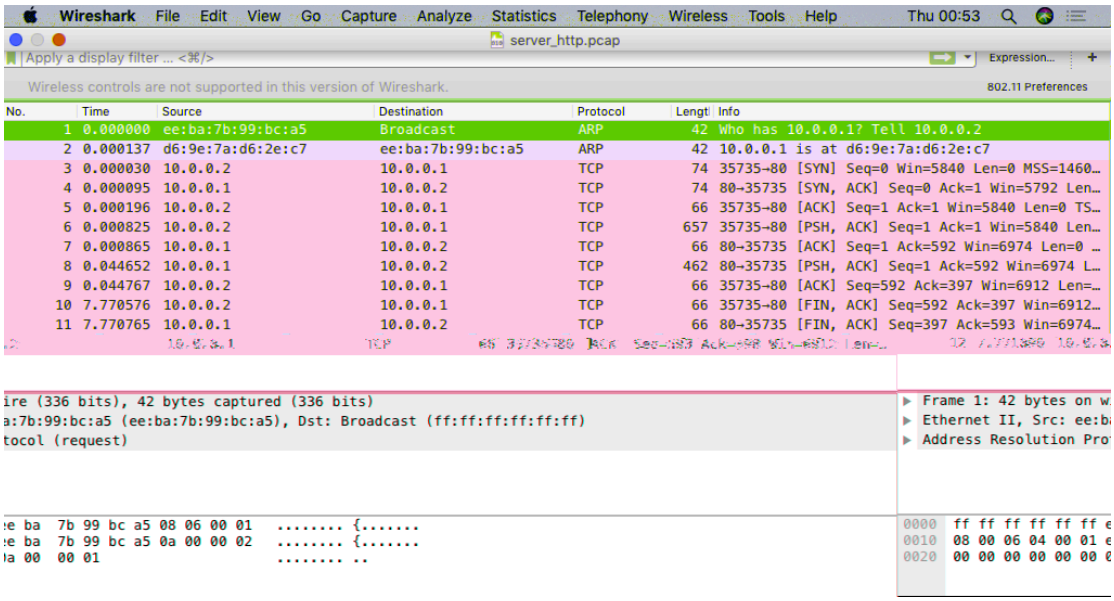
CHƯƠNG 2
BUỔI THỰC HÀNH SỐ 2

ươ , ẽ ớ ệ ề , ộ ụ ắ ạ ỗ ợ . C ụ ọ ệ ứ ề ả ữ ệ ạ , ẳ ạ : IC , A .... , ế ứ ề ề ả ữ ệ ả E II ớ đị ỉ AC ũ đượ ạ ướ ạ ỏ . C ươ ồ ộ : ớ ệ ổ ề ụ ệ ươ ; ứ ử ụ ể ộ ự ạ C 112 ế ợ ớ . C ố ươ ậ ự ủ ố ế ứ ỹ ă ớ .

2.1 GIỚI THIỆU VỀ WIRESHARK

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

cung cấp giao diện thân thiện và thuận lợi cho việc phân tích chi tiết các gói dữ liệu. Giao diện chính của được miêu tả như trong hình 2.1 dưới đây:



H 2.1 G ệ ươ

– *ệ (C)*: chứa các lựa chọn để tương tác với file đang được mở, chẳng hạn: `File, Edit, View, Go...`

– *Bộ ọ (F)*: lọc và hiển thị dữ liệu tương ứng.

– *D ữ ệ đượ (C)*: thể hiện thông tin chi tiết của các gói dữ liệu bắt được như: `source, destination, protocol, length, info…`

– *ế ủ ữ ệ (D):* số thứ tự frame, chiều dài frame, khuôn dạng frame, khuôn dạng gói tin IP, giao thức tầng ứng dụng…

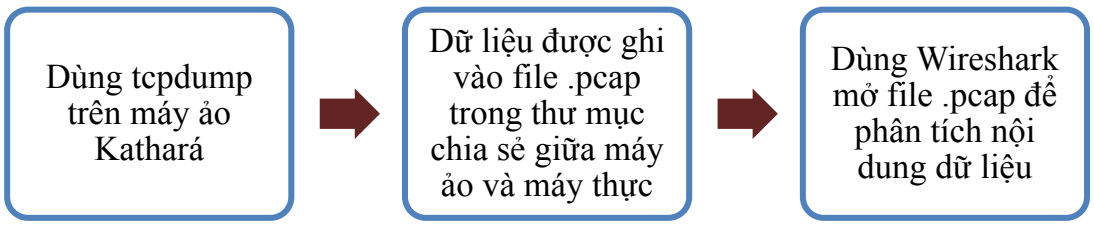
– *ộ ủ ữ ệ :* hiển thị bằng mã HEX và mã ASCII

2.2 VAI TRÒ CỦA WIRESHARK

Công cụ không thể được cài đặt trực tiếp trên máy ảo do máy ảo không hỗ trợ giao diện đồ họa cho người dùng.

Trên máy ảo , sử dụng công cụ `tcpdump` để bắt các gói tin (packet sniffer) và cho phép ghi nhận thông tin của dữ liệu bắt được vào file (`.pcap`). Công cụ này đơn giản hơn Wireshark và không có giao diện đồ họa. Không gian lưu trữ file (`.pcap`) được chia sẻ chung giữa máy ảo và máy thực.

Trên máy thực, truy cập vào thư mục chứa file (`.pcap`) và sử dụng để mở file xem thông tin chi tiết. Nhờ vào giao diện đồ họa thân thiện của mà công việc phân tích gói tin (định dạng, giao thức, địa chỉ, nội dung...) trở nên dễ dàng hơn. Quy trình sử dụng trong phần *ự ạ C 112* có thể được miêu tả như hình 2.2 sau:

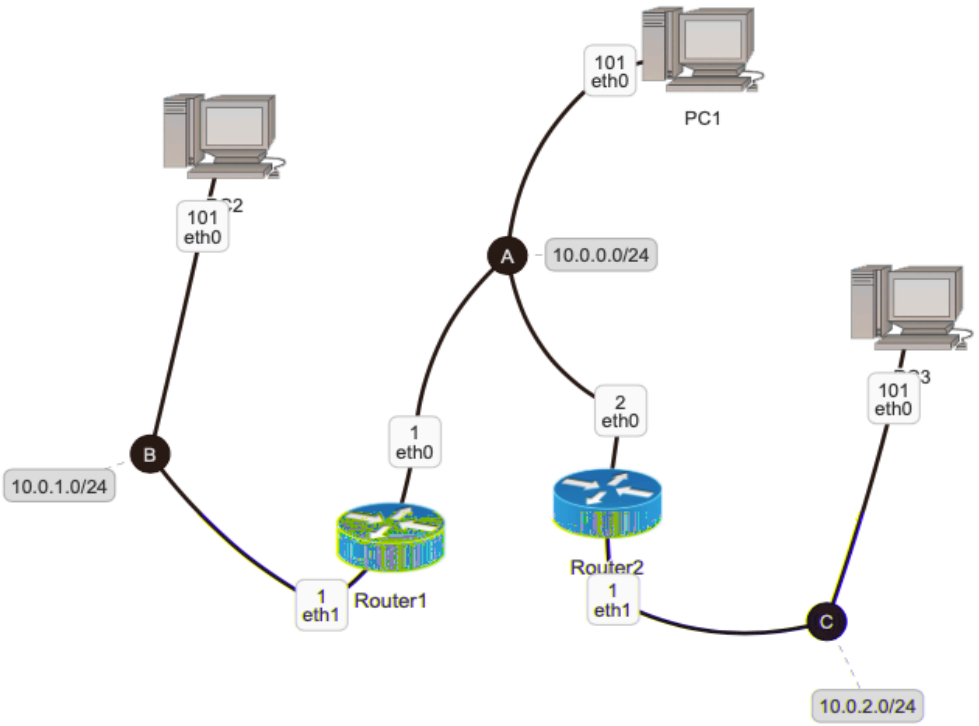


H 2.2 C ứ ụ ự ạ C 112

2.3 BÀI TẬP THỰC HÀNH

2.3.1 Bài tập 5

ụ : Mô phỏng mạng ảo, cài đặt bảng vạch đường tĩnh và khảo sát giao thức ICMP bằng . Các bước thực hiện *B ậ 5* được trình bày chi tiết như sau:



H 2.3 ạ ử ụ B ậ 5

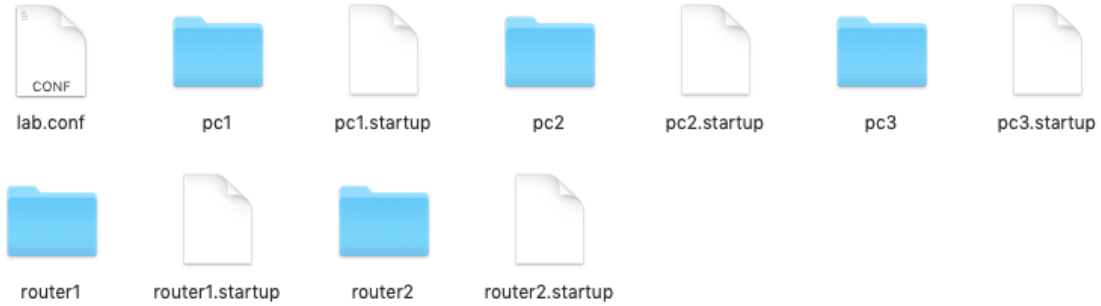
1) Quan sát mô hình mạng cần xây dựng và nhận diện các thiết bị, giao diện với các địa chỉ IP được gán trên các máy ảo.

2) Tạo thư mục *B 5* trong workspace của sinh viên. Thư mục sẽ này chứa các thư mục con và các file cấu hình (`.startup, lab.conf`) theo cấu trúc quy định của .

   Trên máy thực, di chuyển đến thư mục *B 5* bằng lệnh

   ```
   cd /home/student/your_workspace/BaiTap5
   ```

   Cấu trúc thư mục *B 5* được miêu tả như hình 2.4



H 2.4 C ư ụ ệ ư ụ B 5

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
```

4) Trên file *pc1.startup* chứa nội dung được miêu tả 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
```

`route add -net <Network Address> gw <Gateway Address>` cho phép thêm thông tin vạch đường theo dạng tĩnh tới 1 mạng trên một thiết bị.

5) Thêm thông tin vạch đường đến nhánh LAN A, nhánh LAN C trên `pc2.startup` và thêm thông tin vạch đường đến nhánh LAN A, nhánh LAN B trên `pc3.startup`

6) Thêm thông tin vạch đường trên `router1.startup` và `router2.startup` bằng lệnh `route add -net` đã được hướng dẫn nhằm giúp cho `router1` biết đường đi tới LAN C và `router2` 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
```

7) Khởi động mạng ảo *B 5*. Kiểm tra bảng vạch đường (bằng lệnh `route`) trên từng thiết bị mạng (máy ảo).

   Nếu bảng vạch đường của máy ảo nào đó bị sai, thực hiện:

– Kiểm tra lại cấu hình mạng của máy ảo đó bằng lệnh `ifconfig`.

– Tắt máy ảo (`lcrash <may_ao>`) và chỉnh sửa lại chỗ sai trước khi khởi động lại máy ảo (`lstart <may_ao>`)

– Đôi khi, việc khởi động lại toàn bộ mạng ảo (`lrestart`) nên được thực hiện sau khi đã chỉnh xong lỗi sai cho thao tác cấu hình của 1 máy ảo.

8) Trường hợp bảng vạch đường của các thiết bị đều đúng, trên `pc2`, `router1` và `router2` lần lượt thực hiện lệnh `tcpdump` với cú pháp như sau:

```
tcpdump -s 1536 -w /hostlab/BT5_pc2.pcap
```
(ả 2)

`tcpdump -s 1536 -w /hostlab/BT5_router1.pcap` *(ả 1)*

`tcpdump -s 1536 -w /hostlab/BT5_router2.pcap` *(ả 2)*

Thông tin về các gói tin bắt được trên từng máy ảo được lưu vào các file `.pcap`. Các file này trong thư mục `/hostlab` của máy ảo và có thể được truy cập đến từ máy thực.

9) Trên `pc3` thực hiện gửi dữ liệu đến `pc2` bằng lệnh:

`ping 10.0.1.101`

và chờ khoảng 10 giây, sau đó dừng lệnh `ping` lại.

Dừng các lệnh `tcpdump` trên `pc2`, `router1` và `router2` lại.

10) Trên máy thực, mở file `BT5_pc2.pcap` bằng . Chọn khung vật lý (physical frame) số 3 và trả lời các câu hỏi sau đây:

– Toàn bộ khung số 3 có kích thước là bao nhiêu (Bytes)?

– Chọn *H I C* 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?

  ✓ Nội dung thông điệp của giao thức này là gì? Thông điệp này có độ dài bao nhiêu (Bytes)?

– Chọn *H I 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 *H* của thông điệp IP là bao nhiêu? Phần *H* bao gồm những trường (fields) nào? Mỗi trường có độ dài bao nhiêu?

  ✓ Trường có độ dài là bao nhiêu (Bytes). Hãy lý giải tại sao có độ dài như vậy?

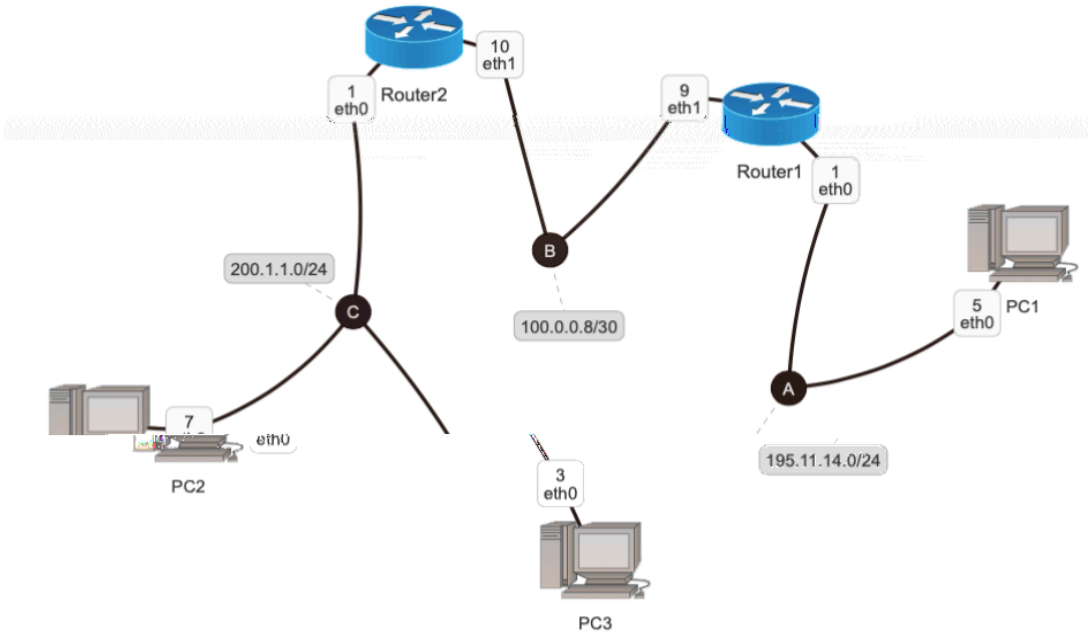
– Chọn *H E II* và cho biết:

  ✓ 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 mang giá trị (hexadecimal) bằng bao nhiêu? Thông tin thể hiện là gì?
- ✓ Hãy chỉ ra trường của khung Ethernet II? Trường này có độ dài bằng bao nhiêu (Bytes)?

11) Hủy mạng ảo bằng lệnh `lwipe` sau khi đã thực hiện xong *B* *ậ* *5*

2.3.2 Bài tập 6



H *2.5* *ạ* *ủ* *B* *ậ* *6*

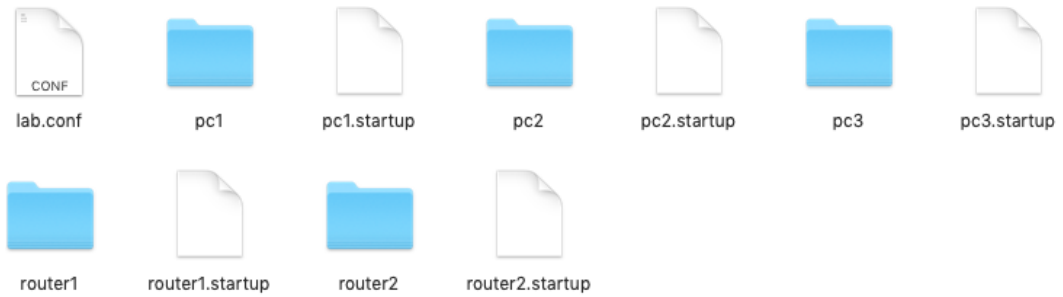
ụ : Mô phỏng mạng ảo, cài đặt bảng vạch đường tĩnh và khảo sát giao thức ARP. Các bước thực hiện *B* *ậ* *6* được trình bày chi tiết như sau:

1) Quan sát mô hình mạng cần xây dựng và nhận diện các thiết bị, giao diện với các địa chỉ IP được gán trên các máy ảo.
2) Tạo thư mục *B* *6* trong workspace của sinh viên. Thư mục sẽ này chứa các thư mục con và các file cấu hình (`.startup, lab.conf`) theo cấu trúc quy định của .

   Trên máy thực, di chuyển đến thư mục *B* *6* bằng lệnh

   ```
   cd /home/student/your_workspace/BaiTap6
   ```

Cấu trúc thư mục *B* *6* được miêu tả như hình 2.6



H *2.6 C* *ư* *ụ* *ệ* *ư* *ụ B* *6*

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

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

4) Trên file *pc1.startup* để vạch đường mặc nhiên thì sẽ chứa nội dung được miêu tả như sau

```
ifconfig eth0 195.11.14.5/24 up
route add default gw 195.11.14.1
```

Trên file `pc2.startup` để vạch đường mặc nhiên sẽ chứa nội dung được miêu tả như sau

```
ifconfig eth0 200.1.1.7/24 up
route add default gw 200.1.1.1
```

Thực hiện tương tự trên `pc3.startup`

Lưu ý: các nội dung vạch đường mặc nhiên (`route add default`) có thể thay thế bằng vạch đường tĩnh (`route add -net`)

5) Trên file `router1.startup` và `router2.startup` cũng thực hiện thêm thông tin vạch đường tĩnh sao cho `router1` biết hướng đi tới LAN C và `router2` biết hướng đi tới LAN A.

Nội dung file `router1.startup` có thể được trình bày như sau:

```
ifconfig eth0 195.11.14.1/24 up
```

```
ifconfig eth1 100.0.0.9/30 up
route add -net 200.1.1.0/24 gw 100.0.0.10
```

6) Khởi động mạng ảo *B* *6*. Kiểm tra bảng vạch đường (lệnh `route`) và địa chỉ IP của các giao diện mạng (lệnh `ifconfig`) trên từng máy ảo để đảm bảo tính đúng đắn của mô hình mạng *B* *ậ* *6*. Nếu có sai sót, thực hiện các thao tác điều chỉnh theo hướng dẫn đã trình bày trong *7)* của *B* *ậ* *5*.

2.3.2.1. G *ứ* *A* *ữ* *2* *ế* *ị* *ạ* *A* *C*

7) Trên máy ảo `pc3`, `pc2` và `router2`, lần lượt dùng lệnh `arp`. Nhận xét kết quả

8) Lần lượt thực hiện lệnh `tcpdump` với cú pháp như sau:

`tcpdump -s 1536 -w /hostlab/BT6_pc2_A.pcap (` *ả* *2)*

`tcpdump -s 1536 -w /hostlab/BT6_router1_A.pcap (` *ả* *1)*

`tcpdump -s 1536 -w /hostlab/BT6_router2_A.pcap (` *ả* *2)*

9) Trên `pc3` thực hiện gửi dữ liệu đến `pc2` bằng lệnh:

```
ping 200.1.1.7
```

và chờ khoảng 10 giây, sau đó dừng lệnh `ping` trên `pc3` lại.

Dừng các lệnh `tcpdump` trên `pc2`, `router1` và `router2` lại.

10) Trên `pc3` thực hiện lại lệnh `arp` và nhận xét kết quả hiển thị.

Lưu ý sự thay đổi so với kết quả ở 7). Lý giải cho sự thay đổi này.

Ghi nhận kết quả hiển thị để so sánh với 10) ở mục *2.3.2.2*.

11) Trên `pc2`, thực hiện lại lệnh `arp` và nhận xét kết quả hiển thị.

Lưu ý sự thay đổi so với kết quả ở bước số 7). Lý giải cho sự thay đổi này.

12) Trên `router2`, thực hiện lại lệnh `arp` và nhận xét kết quả hiển thị.

Ghi nhận kết quả hiển thị để so sánh với bước 12) ở mục *2.3.2.2*.

13) Trên máy thực, dùng mở file `BT6_router2_A.pcap`, chọn khung vật lý số thứ tự 1. Trả lời các câu hỏi sau đây:

– Toàn bộ khung số thứ tự 1 có kích thước là bao nhiêu (Bytes)?

– Chọn *H* *A* và cho biết:

  ✓ Trường có giá trị (hexadecimal) là bao nhiêu? Giá trị của trường này thể hiện thông tin gì? Trường này còn có thể có giá trị (hexadecimal) là bao nhiêu nữa và 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 *H E 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 *H A*
- ✓ Trường mang giá trị (hexadecimal) bằng bao nhiêu? Thông tin thể hiện là gì?

14) Hủy mạng ảo bằng lệnh `lwipe` sau khi đã thực hiện xong phần *2.3.2.1*

2.3.2.2. G ứ A ừ 2 ế ị ạ A

7) Mở lại mạng ảo bằng lệnh `lstart`. Trên máy ảo `pc1` và `router1`, lần lượt dùng lệnh `arp`, nhận xét kết quả hiển thị.

8) Lần lượt thực hiện lệnh `tcpdump` với cú pháp như sau:

`tcpdump -s 1536 -w /hostlab/BT6_pc1_B.pcap (` *ả 1)*

`tcpdump -s 1536 -w /hostlab/BT6_router1_B.pcap (` *ả 1)*

`tcpdump -s 1536 -w /hostlab/BT6_router2_B.pcap (` *ả 2)*

9) Trên `pc3` thực hiện gửi dữ liệu đến `pc1` bằng lệnh:

```
ping 195.11.14.5
```

và chờ khoảng 10 giây, sau đó dừng lệnh `ping` trên `pc3` lại.

Dừng các lệnh `tcpdump` trên `pc1`, `router1` và `router2`.

10) Trên `pc3` thực hiện lại lệnh `arp` và nhận xét kết quả hiển thị. Lưu ý: so sánh với 10) ở phần *2.3.2.1*.

11) Trên `router2`, thực hiện lại lệnh `arp` và nhận xét kết quả hiển thị. Lưu ý: so sánh với 12) ở phần *2.3.2.1*.

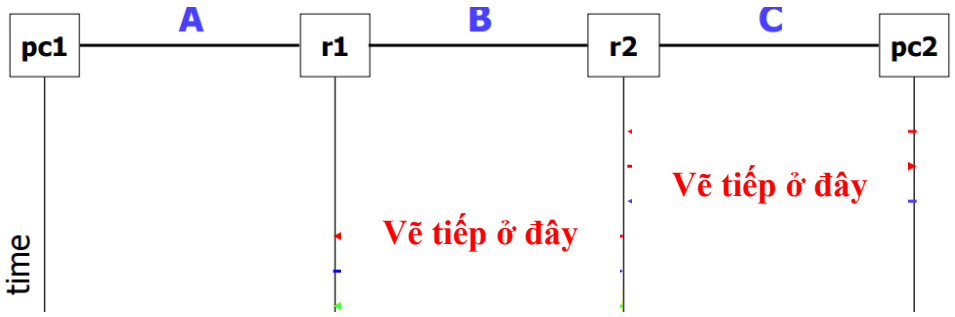
12) Trên `router1`, thực hiện lại lệnh `arp` và nhận xét kết quả hiển thị.

13) Trên `pc1`, thực hiện lại lệnh `arp` và nhận xét kết quả hiển thị. Lưu ý: so sánh với thông tin hiển thị của máy `pc1` tại 7) ở phần *2.3.2.2*.

14) Trên máy thực, dùng Wireshark mở file `BT6_Router1_B.pcap`, chọn khung vật lý số thứ tự 1.

– Trả lời các câu hỏi giống như 13) ở phần *2.3.2.1* đã trình bày.

– Vẽ sơ đồ tuần tự (sequence diagram) thể hiện vai trò của giao thức ARP trong việc truyền tải dữ liệu từ `pc3` đến `pc1` bằng lệnh `ping`



H *2.7* *ơ đồ* *à* *ự* *ể* *ễ* *ạ* *độ* *ủ* *ứ* *A* *ừ* *1 đế* *3*

15) Hủy mạng ảo bằng lệnh `lwipe` sau khi đã thực hiện xong *2.3.2.2*

2.3.2.3. G *ứ* *A* *ớ* *đị* *ỉ* *ầ* *ả* *ạ* *đườ*

– Trên `pc1`, gửi dữ liệu đến *G* *D* (địa chỉ ngoài mạng ảo) bằng lệnh

```
ping 8.8.8.8
```

– Ghi nhận kết quả hiển thị khi dùng lệnh `arp` trên `pc1` và `router1`. Nhận xét kết quả này.

2.3.2.4. G *ứ* *A* *ớ* *đị* *ỉ* *ộ* *ạ* *A* *ứ* *ụ*

– Trên `pc1`, gửi dữ liệu đến *195.11.14.200* (địa chỉ không tồn tại có thể được cấp phát trong nhánh LAN A) bằng lệnh

```
ping 195.11.14.200
```

– Ghi nhận kết quả hiển thị khi dùng lệnh `arp` trên `pc1` và `router1`. Nhận xét kết quả này.

16) Hủy mạng ảo bằng lệnh `lwipe` sau khi đã thực hiện xong *B* *ậ* *6*.

2.3.3 Bài tập 7

ụ : Mô phỏng mạng ảo, cài đặt bảng vạch đường tĩnh với nhiều thông tin vạch đường tĩnh. Các bước thực hiện *B* *ậ* *7* được trình bày chi tiết như sau:

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.

2) Tạo thư mục *B* *7* trong workspace của sinh viên.

3) Soạn thảo nội dung mô tả hình thái mạng theo thiết kế trên file *Lab.conf*

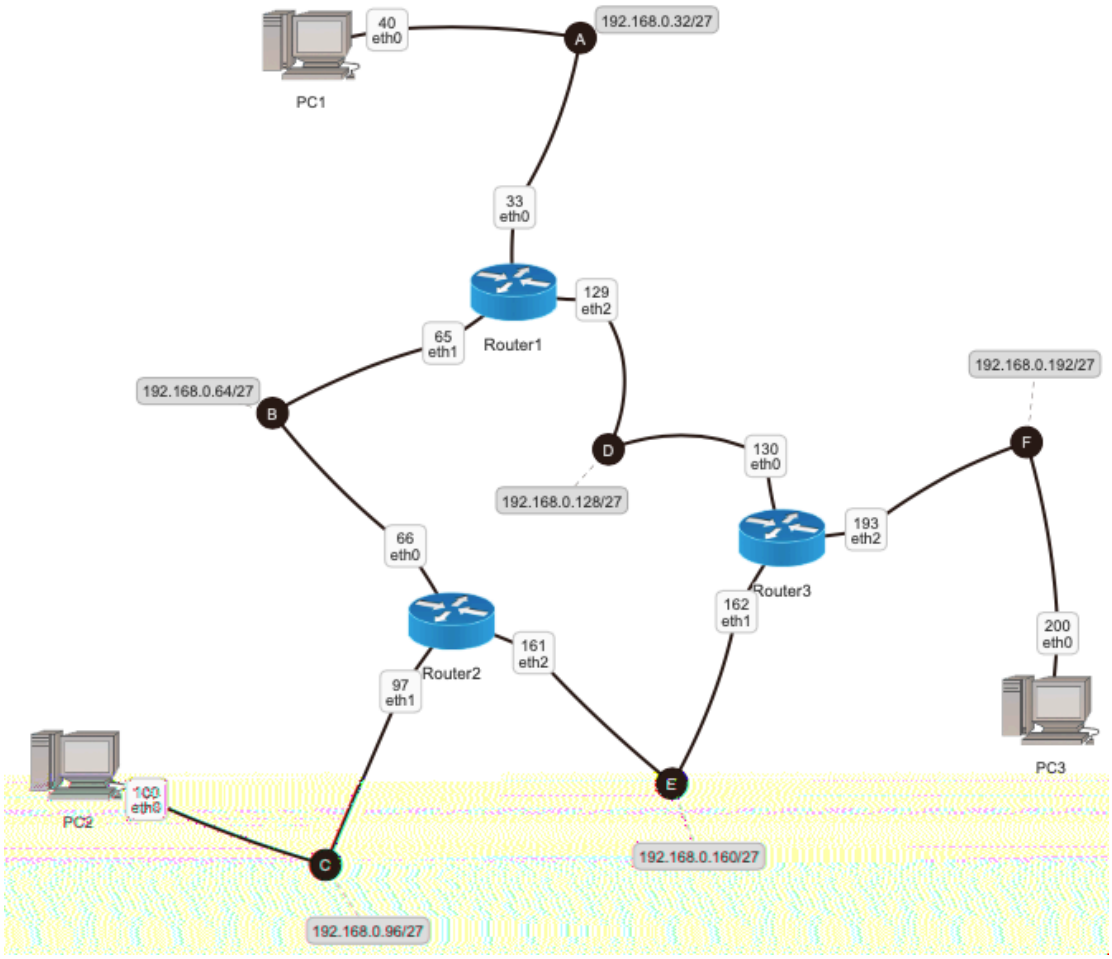
4) Đối với các file `pc1.startup`, `pc2.startup` và `pc3.startup`: thực hiện vạch đường mặc nhiên thông qua các Router tương ứng trong nhánh mạng.

5) Đối với các file `router1.startup`, `router2.startup` và `router3.startup`: thực hiên vạch đường tĩnh và vạch đường mặc nhiên (nếu cần)

6) Khởi động mạng ảo *B* *7*. Kiểm tra bảng vạch đường (bằng `route`) và địa chỉ IP của các giao diện mạng (bằng `ifconfig`) trên từng máy ảo để đảm bảo tính đúng đắn của mô hình mạng *B* *ậ* *7*.

   Kiểm tra tính liên thông giữa `pc1`, `pc2` và `pc3` trong mạng (bằng `ping`).

7) Hủy mạng ảo bằng lệnh `lwipe` sau khi đã thực hiện xong *B* *ậ* *7*



H *2.8* *ạ* *ử* *ụ* *B* *ậ* *7*