**Mssv: B2012046**

**Họ Tên: Đỗ Khánh Toàn**

**Nhóm 01**

**CT112-01 BÀI THỰC HÀNH 2**

**PHÂN TÍCH DỮ LIỆU MẠNG**

**Lap 5:**

**1,2,3) Đầu tiên khởi tạo 5 file bằng lệnh gedit như sau:**

- lab.conf

pc1[0]=A

pc2[0]=B

pc3[0]=C

router1[0]=A

router1[1]=B

router2[0]=A

router2[1]=C

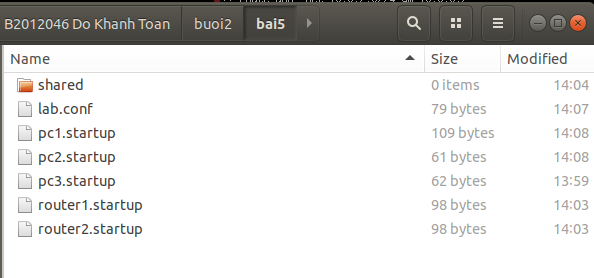
- pc1.startup

- pc2.startup

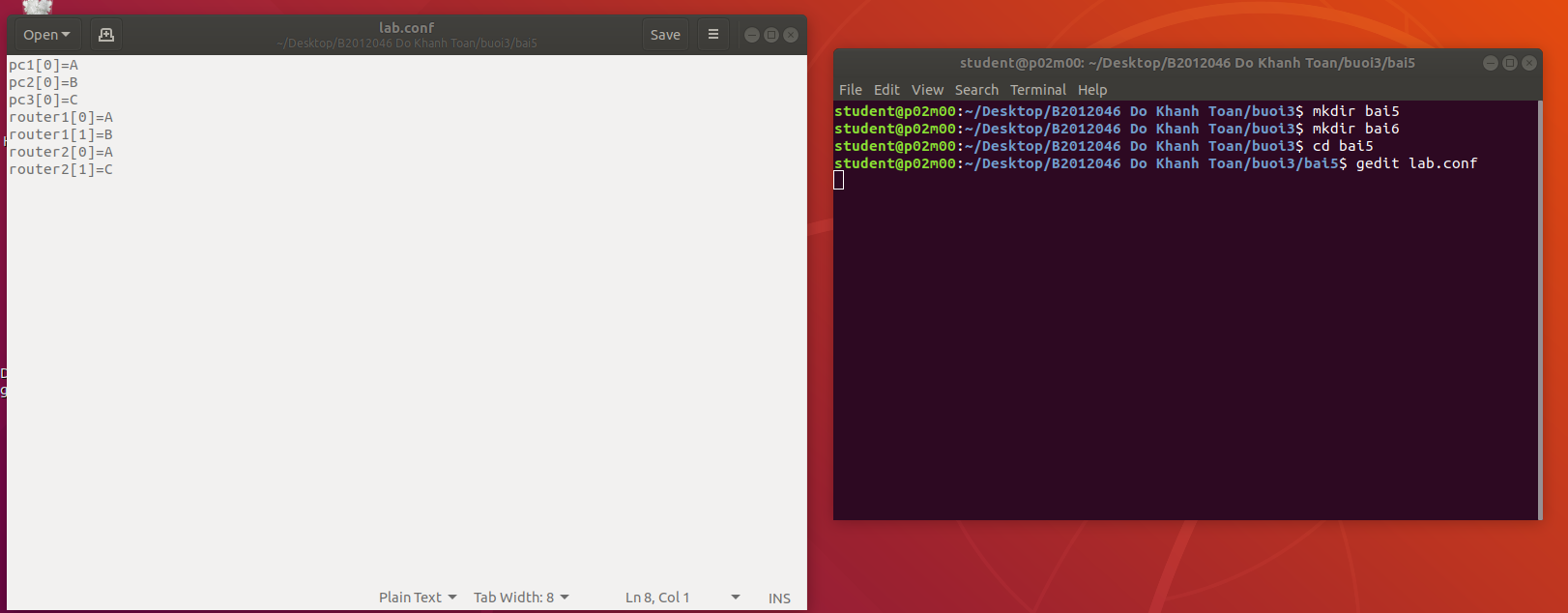
- pc3.startup

- router1.startup

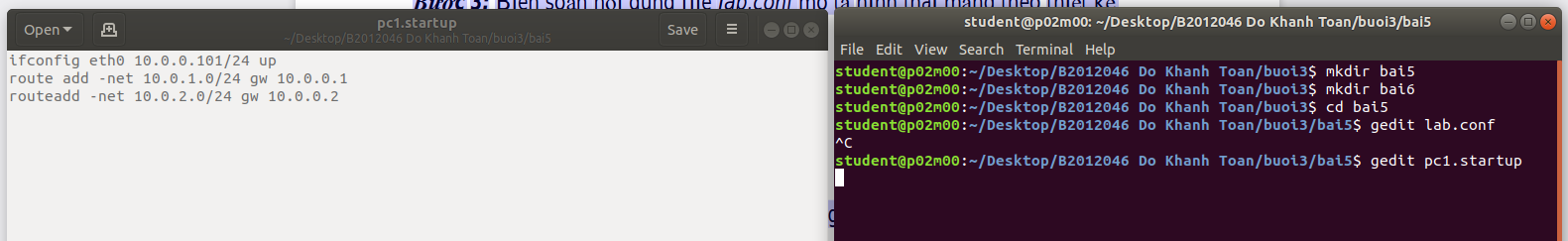
- router2.startup



=> Trên file lab.conf, soạn thảo nội dung mô tả hình thái mạng theo thiết kế

****

**4) Biên soạn pc1.startup bao gồm thông tin vạch đường đến LAN B và C:**

****

**5,6 ) Thực hiện tương tự cho file pc2.startup (thông tin vạch đường đến nhánh**

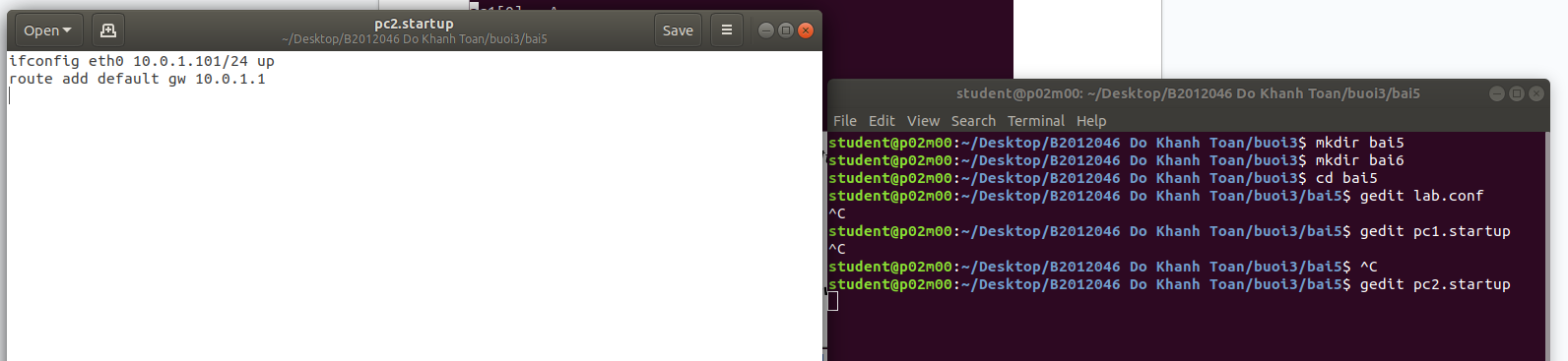
**LAN A, và LAN C) trên và file pc3.startup (thêm thông tin vạch đường đến nhánh**

**LAN A và LAN B)**

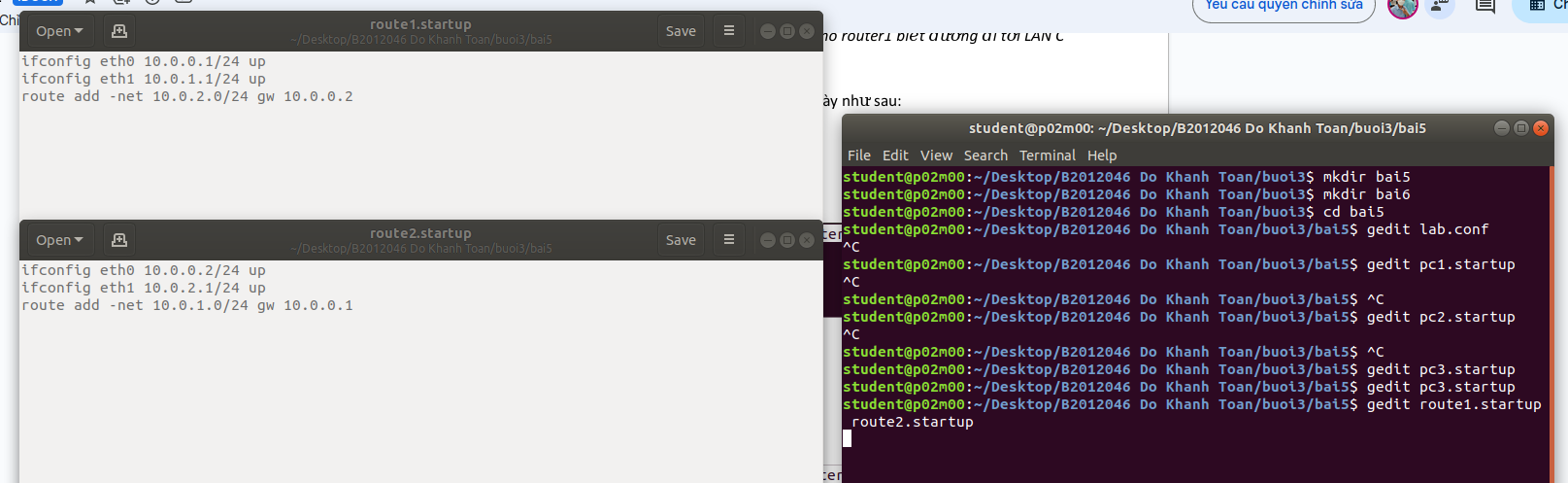
ifconfig eth0 10.0.0.101/24 up

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

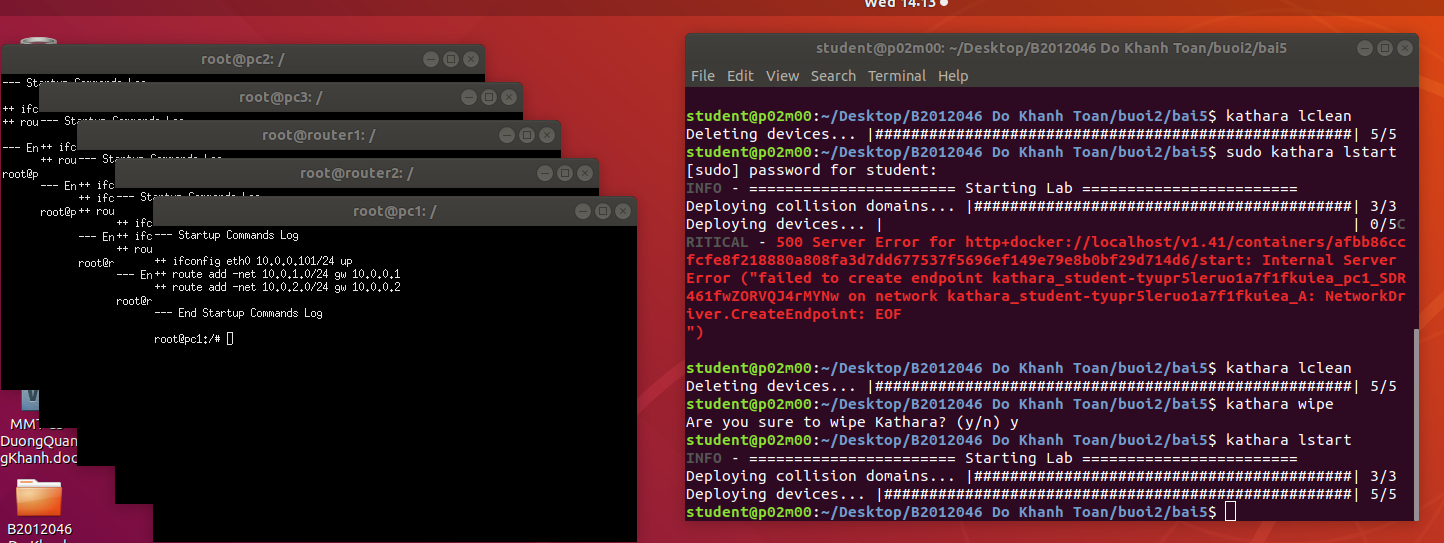
****

**7) 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**

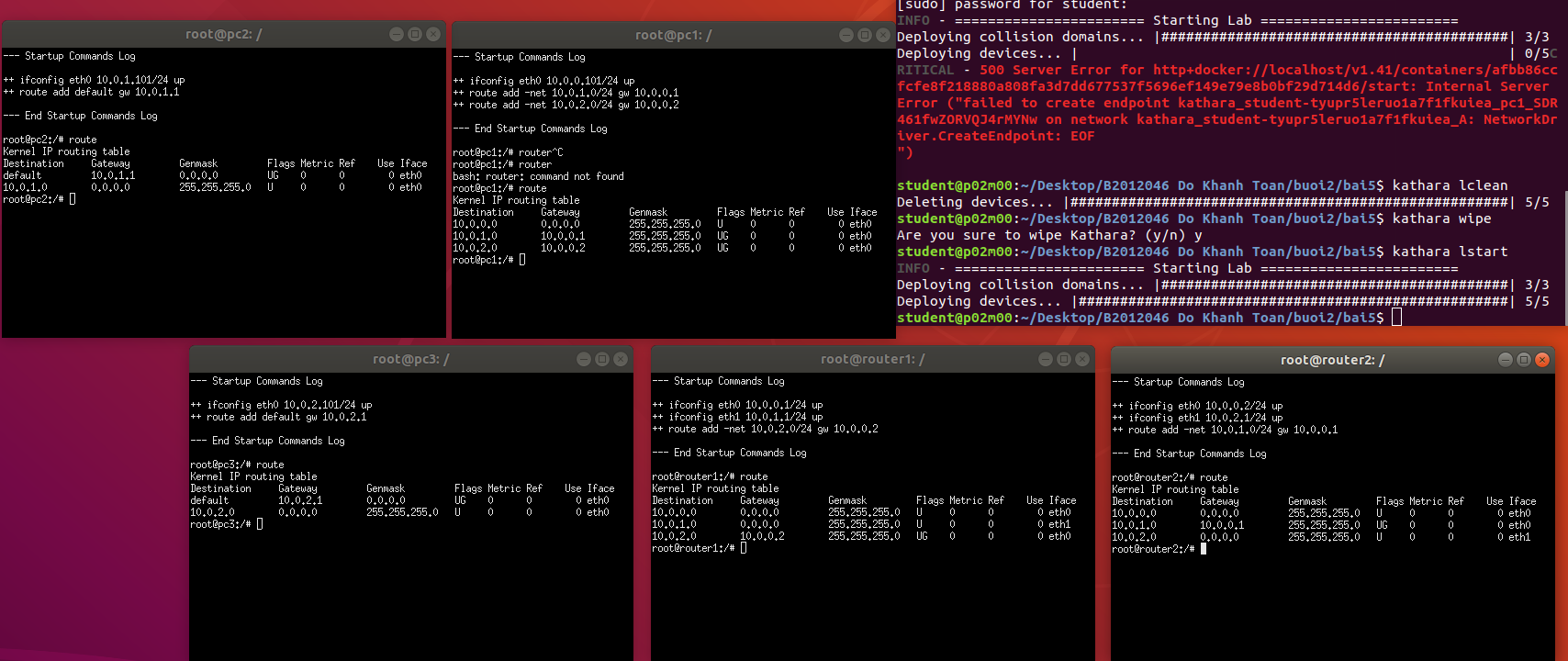
****

Ở đây bị lỗi màu đỏ như bên dưới nên em dùng lệnh kathara wipe để fix

sau khi fix xong chạy lệnh kathara lstart kết quả như hình bên dưới

****

Kiểm tra bảng vạch đường (bằng lệnh route) trên từng thiết bị mạng (máy ảo).

****

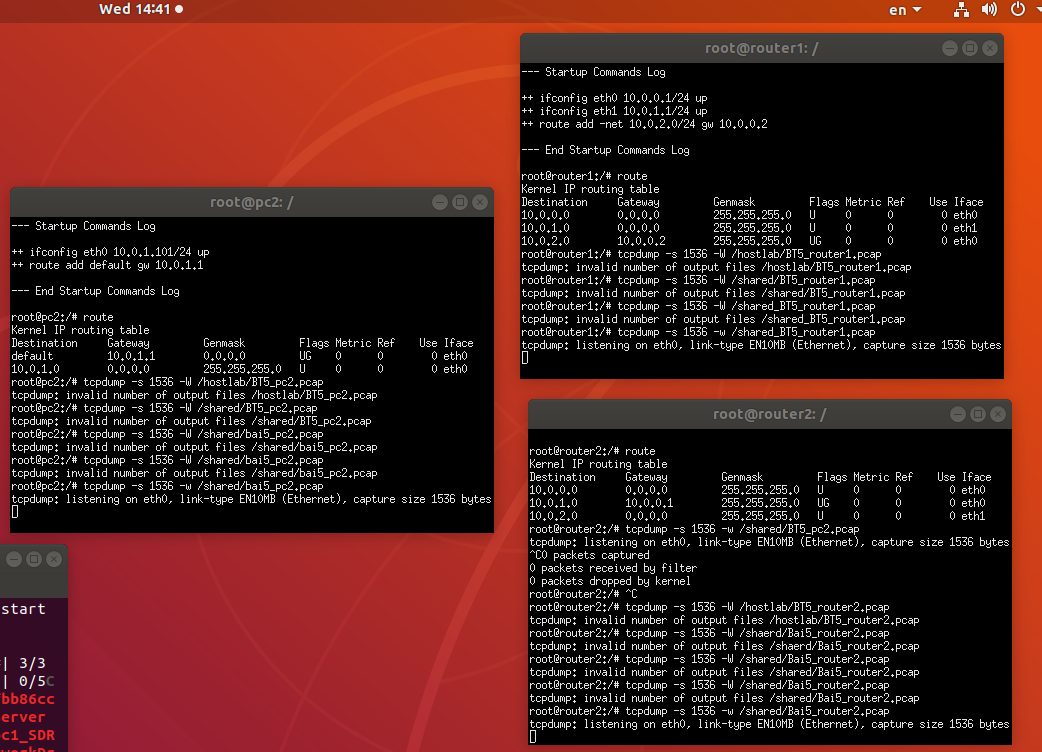
**8) Trường hợp bảng vạch đường của các thiết bị đều đúng, trên pc2, router1**

**và router2 lần lượt thực hiện lệnh tcpdump với cú pháp như sau:**

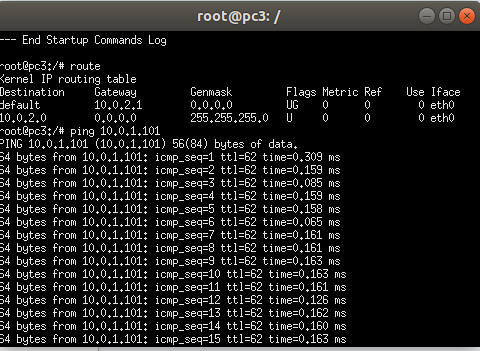
tcpdump -s 1536 -w /shared/BT8\_pc2.pcap (trên máy ảo pc2)

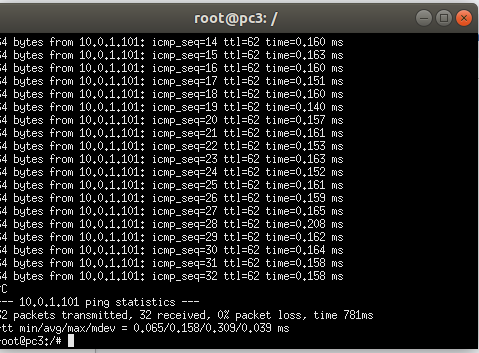
tcpdump -s 1536 -w /shared/BT8\_router1.pcap (trên máy ảo router1)

tcpdump -s 1536 -w /shared/BT8\_router2.pcap (trên máy ảo router2)

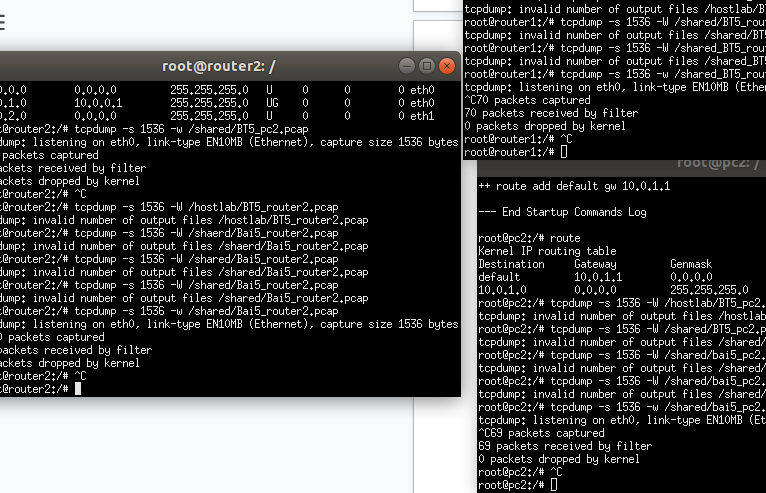
****

**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.**

****

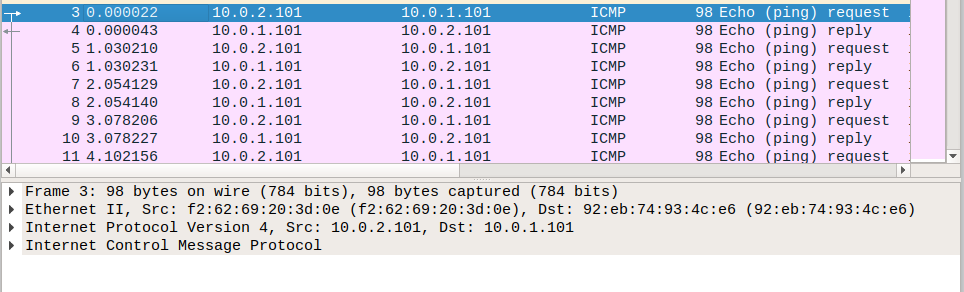
****

**10) Sau đó dừng các máy ảo pc2, router1 , router2 lại**



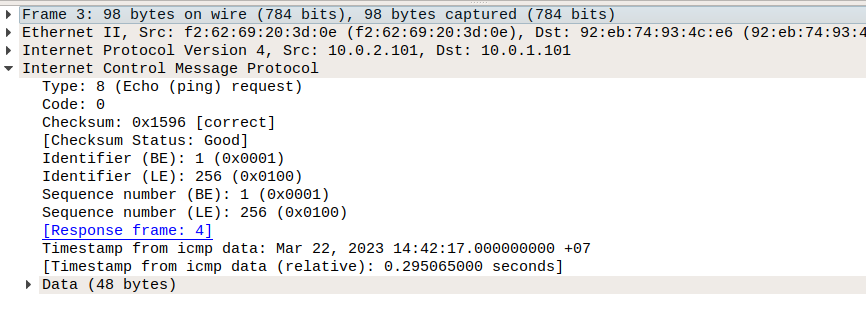
**11) Trên máy thực, mở file BT5\_pc2.pcap bằng Wireshark. Chọn khung vật lý**

**(physical frame) số 3:**

****

=> Toàn bộ khung số 3 có kích thước là 98 bytes

* **Chọn Header Internet Control Message Protocol trong khung và cho biết:**



**Gói tin này sử dụng giao thức gì?**

=> Gói tin này sử dụng giao thức ICMP

**Giao thức này hoạt động trên tầng nào của mô hình OSI?**

=> Giao thức này hoạt động trên tầng Tầng network của mô hình OSI?

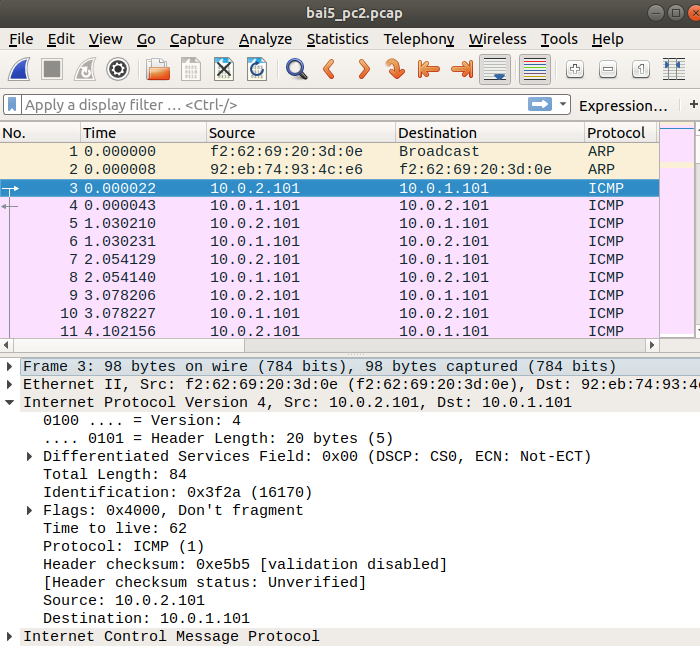
**Nội dung thông điệp của giao thức này là gì?**

=> Nội dung thông điệp của giao thức này là gì giao thức này được các thiết bị mạng như router dùng để gửi đi các thông báo lỗi chỉ ta một dịch vụ có tồn tại hay không hoặc một địa chỉ host hay router có tồn tại hay không. ICMP cũng có thể được sử dụng để chuyển tiếp các thông điệp truy vấn

**Thông điệp này có độ dài bao nhiêu (Bytes)?**

=> Thông điệp này có độ dài là 48 bytes

* **Chọn Header Internet Protocol Version 4 và cho biết:**

****

**Địa chỉ IP của máy gửi dữ liệu là bao nhiêu?**

**=>** Địa chỉ IP của máy gửi dữ liệu là 10.0.2.101.

**Địa chỉ IP này là của máy tính nào trong mạng?**

**=>** Địa chỉ IP này là của một máy tính trong mạng có địa chỉ mạng là 10.0.2.0/24.

**Địa chỉ IP của máy nhận dữ liệu là bao nhiêu?**

**=>** Địa chỉ IP của máy nhận dữ liệu là 10.0.1.101.

**Địa chỉ IP này là của máy tính nào trong mạng?**

**=>** Địa chỉ IP này là của một máy tính trong mạng có địa chỉ mạng là 10.0.1.0/24.

**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?**

**=>** Định danh (ID) của gói tin IP này là 0x3f2a (16170) (dạng hexadecimal). Định danh của một gói tin có ý nghĩa là một giá trị duy nhất được gán cho mỗi gói tin để có thể định danh và tái lập lại gói tin trong trường hợp gói tin bị mất hoặc bị hư hỏng trong quá trình truyền.

**Độ dài phần Header của thông điệp IP là bao nhiêu? Phần Header bao gồm những trường (fields) nào?**

=> Độ dài phần Header của thông điệp IP là 20 bytes (5). Phần Header bao gồm các trường sau:

Version: 4 bits

Header Length: 4 bits

Differentiated Services Field: 8 bits

Total Length: 16 bits

Identification: 16 bits

Flags: 3 bits

Fragment Offset: 13 bits

Time to Live: 8 bits

Protocol: 8 bits

Header Checksum: 16 bits

Source IP Address: 32 bits

Destination IP Address: 32 bits

**Mỗi trường có độ dài bao nhiêu?**

=> Trường Total Length có độ dài là 84 bytes.

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

Đây là tổng số bytes của toàn bộ gói tin IP, bao gồm cả phần Header và phần Payload (dữ liệu được gửi). Trường này có độ dài là 16 bits (2 bytes) để có thể biểu diễn giá trị tối đa của 65,535 bytes. Trong trường hợp này, độ dài của gói tin IP là 84 bytes.

* **Chọn Header Ethernet II và cho biết:**

(em quên chụp ảnh mong Thầy thông cảm)

**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 gửi dữ liệu là f2:62:69:20:3d:0e.

=> Địa chỉ MAC này là của máy tính gửi dữ liệu.

**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?**

**=>** Địa chỉ MAC của máy nhận dữ liệu là 92:eb:74:93:4c:e6.

=> Địa chỉ MAC này là của máy tính nhận dữ liệu.

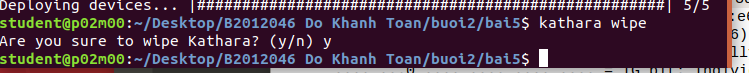
**Trường Type mang giá trị (hexadecimal) bằng bao nhiêu? Thông tin thể hiện là gì?**

**=>** Trường Type mang giá trị hexadecimal bằng 0x0800.

**Hãy chỉ ra trường Payload của khung Ethernet II? Trường Payload này có độ dài bằng bao nhiêu (Bytes)?**

Trường Payload của khung Ethernet II chứa dữ liệu của gói tin IPv4, bao gồm cả tiêu đề và phần dữ liệu. Độ dài của trường Payload phụ thuộc vào độ dài của gói tin IPv4 và có thể được tính bằng cách lấy giá trị của trường Total Length trong tiêu đề IPv4 trừ đi độ dài của tiêu đề IPv4 (20 bytes).

**12) Hủy mạng ảo bằng lệnh lwipe**

****

**Lap 6:**

**1,2,3) Trên file lab.conf, soạn thảo nội dung mô tả hình thái mạng theo thiết kế**

pc1[0]=A

pc2[0]=C

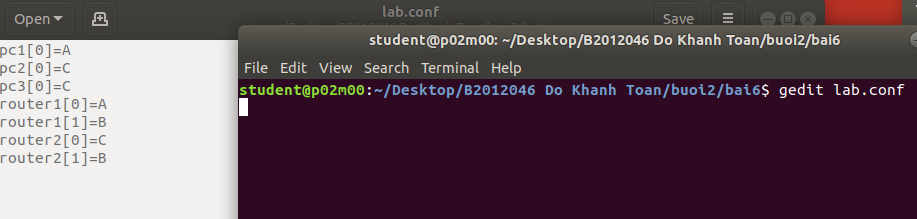
pc3[0]=C

router1[0]=A

router1[1]=B

router2[0]=C

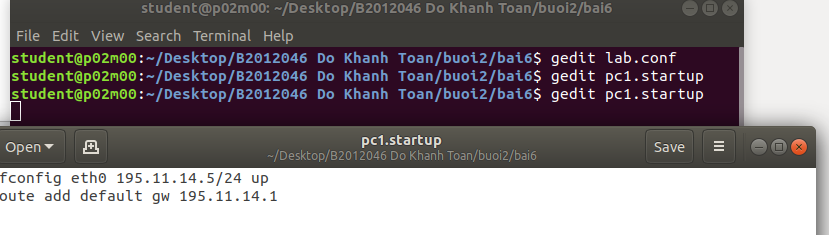
router2[1]=B

****

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

ifconfig eth0 195.11.14.5/24 up

route add default gw 195.11.14.1

****

**5, 6) 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.**

=> Tương tự như vậy tiếp tục Trên file pc2.startup router1.starup và router2.startup 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.

**Trên file pc2.startup:**

ifconfig eth0 200.1.1.7/24 up

route add default gw 200.1.1.1

**Tương tự trên pc3.startup**

ifconfig eth0 200.1.1.3/24 up

route add default gw 200.1.1.1

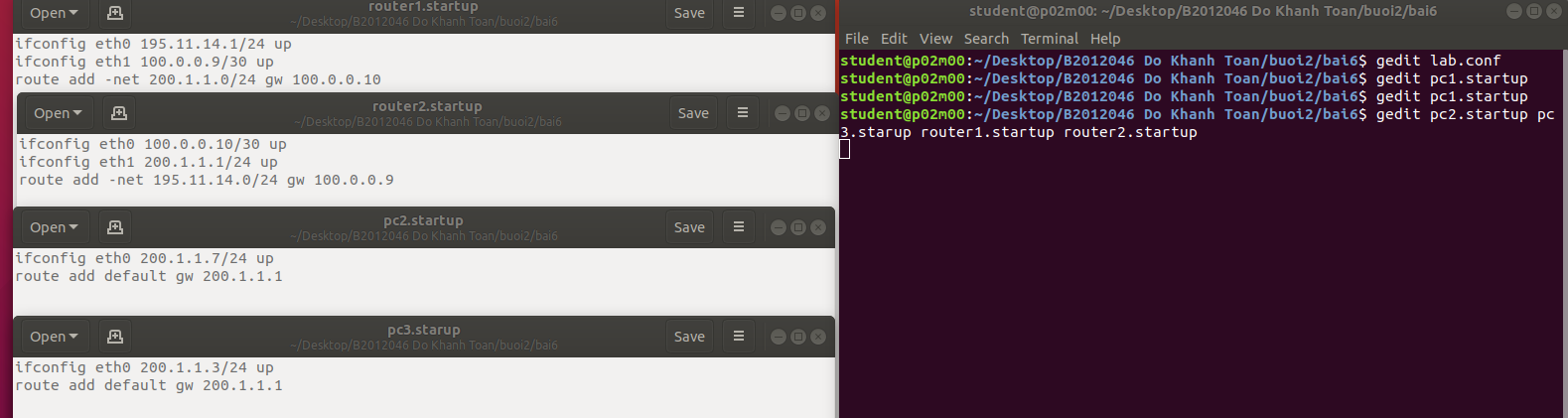
**Trên file router1.startup và router2.startup cũng thực hiện thêm thông tin vạch đường tĩnh sao cho router1 biết hướng đi tới LAN C và router2 biết hướng đi tới LAN A.**

ifconfig eth0 195.11.14.1/24 up

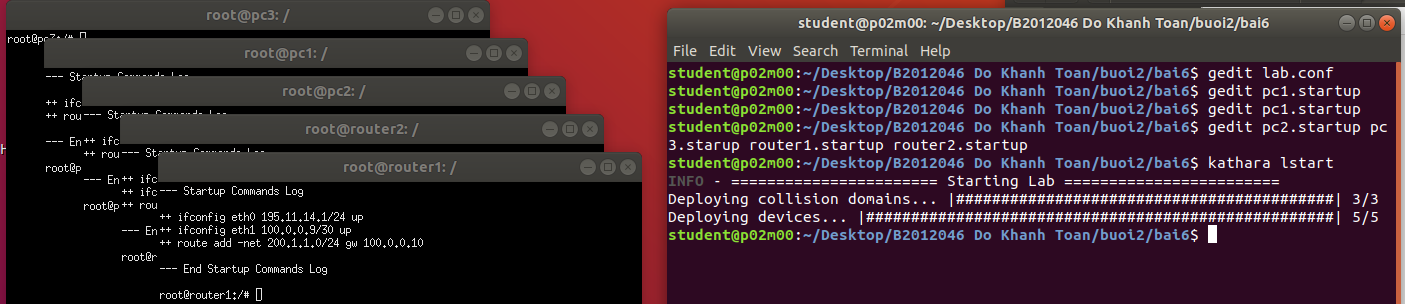
ifconfig eth1 100.0.0.9/30 up

route add -net 200.1.1.0/24 gw 100.0.0.10

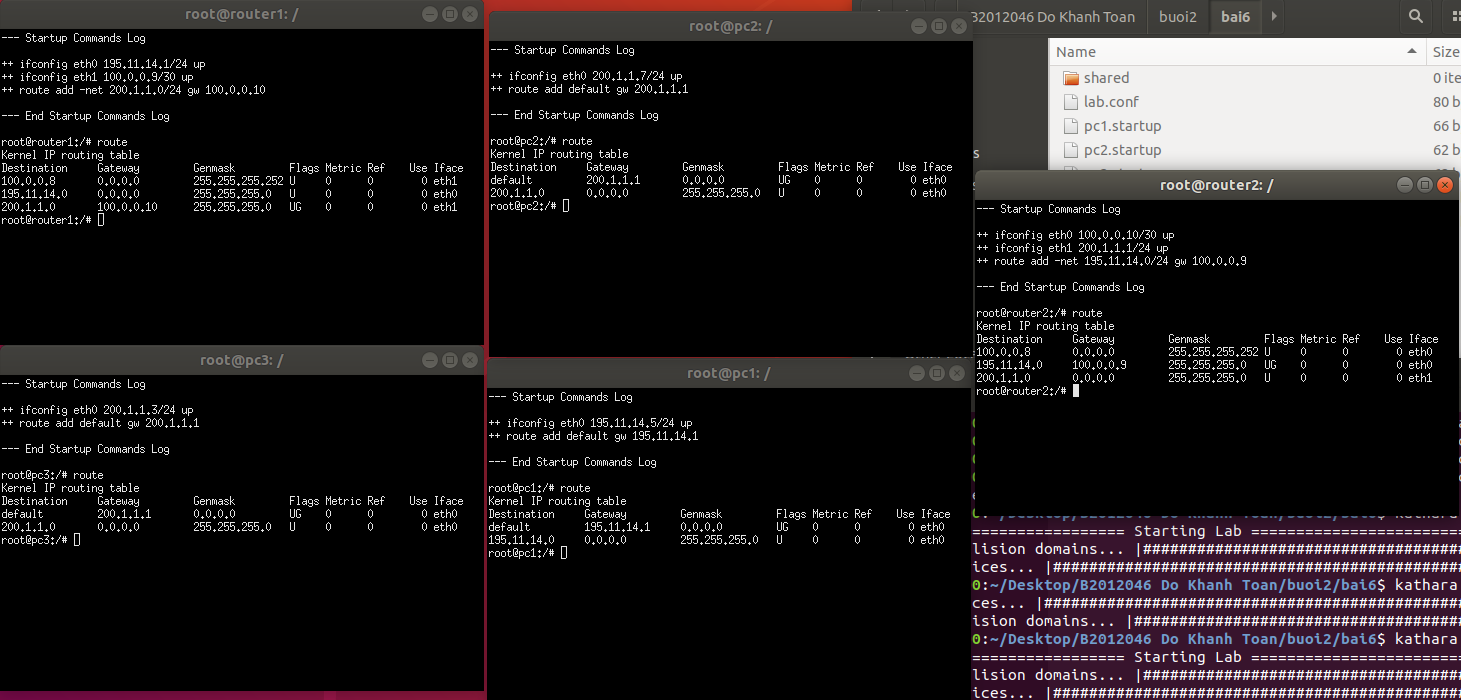
Tất cả được tóm gọn lại như ảnh sau:

****

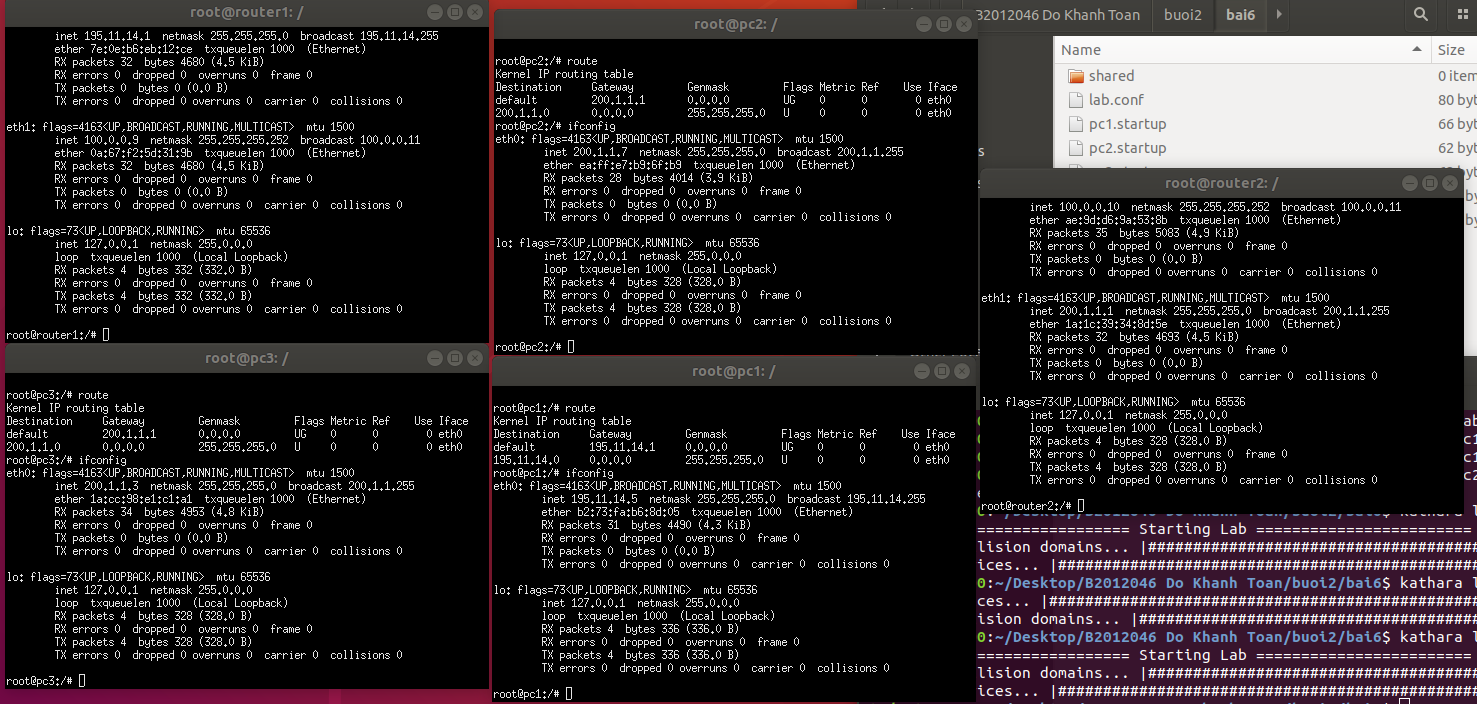
**6) Khởi động mạng ảo BaiTap6. Kiểm tra bảng vạch đường (bằng lệnh route) trên từng thiết bị mạng. Nếu bảng vạch đường của 1 thiết bị nào đó bị sai, kiểm tra lại cấu hình mạng (bằng lệnh ifconfig) của thiết bị đó. Khởi động lại thiết bị hoặc khởi động lại mạng ảo (nếu cần).**

****

**=> route**



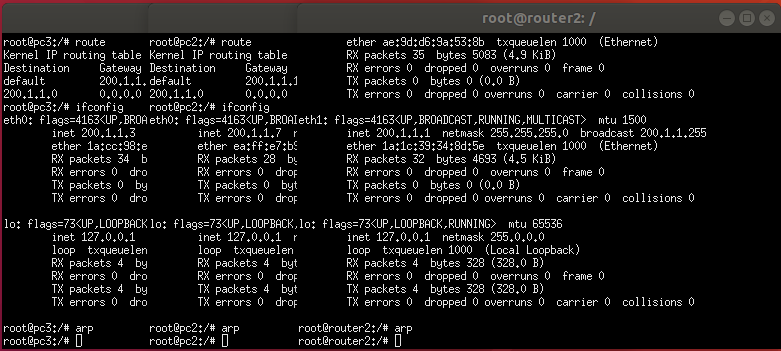
**=> ifconfig**



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

**7A) Trường hợp bảng vạch đường của các thiết bị đều đúng, trên máy ảo pc3, pc2 và router2, lần lượt dùng lệnh arp. Nhận xét kết quả:**

=> Không có gì xảy ra

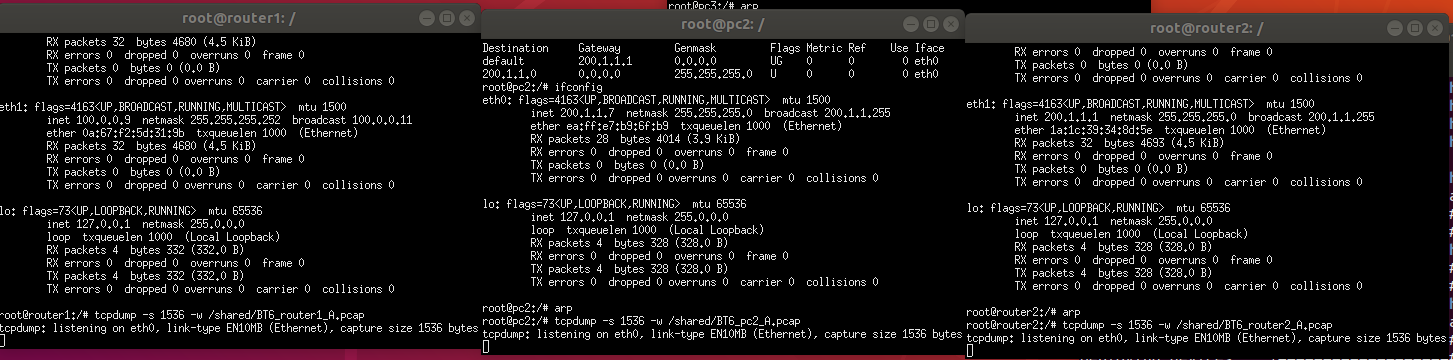


**8A) Lần lượt thực hiện lệnh tcpdump với cú pháp như sau:**

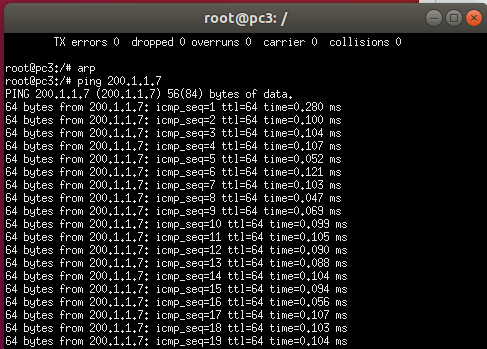
tcpdump -s 1536 -w /shared/BT6\_pc2\_A.pcap (trên máy ảo pc2)

tcpdump -s 1536 -w /shared/BT6\_router1\_A.pcap (trên máy ảo router1)

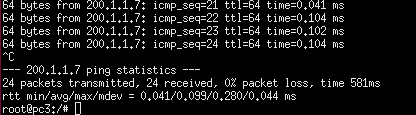
tcpdump -s 1536 -w /shared/BT6\_router2\_A.pcap (trên máy ảo router2)



**9A) Trên pc3 thực hiện gửi dữ liệu đến pc2 bằng lệnh:** ping 200.1.1.7

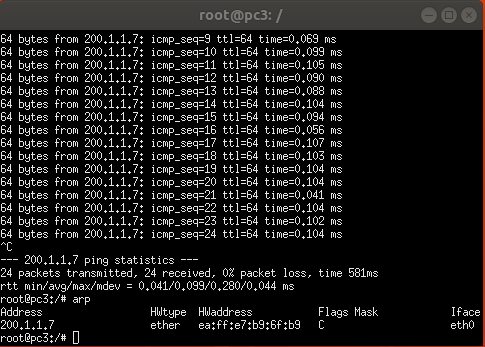
****

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

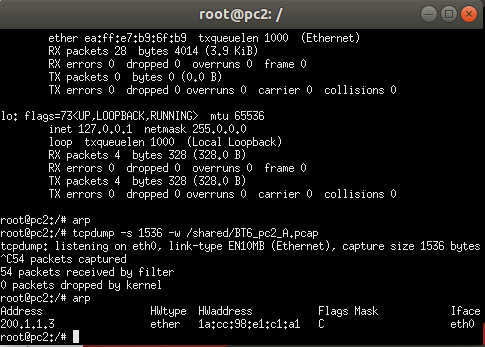
****

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

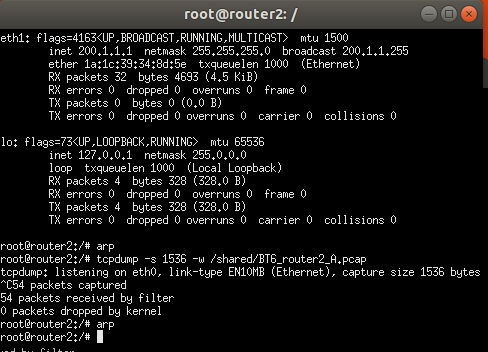
**10A) Trên pc3 thực hiện lại lệnh arp và nhận xét kết quả hiển thị. Lưu ý sự thay đổi so với kết quả ở 7A).**

****

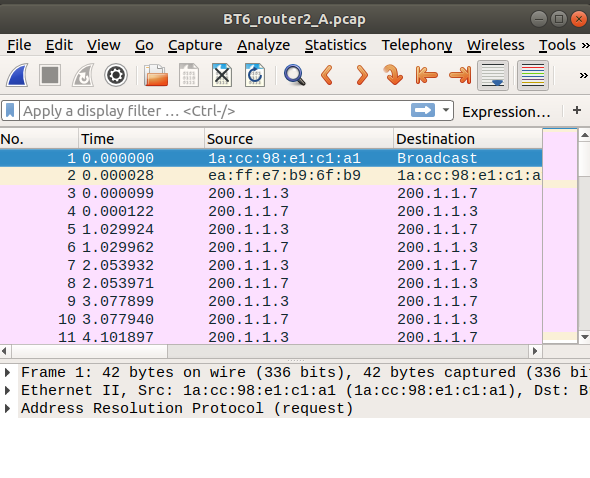
**11A) Trên pc2, thực hiện lại lệnh arp và nhận xét kết quả hiển thị.Lưu ý sự thay đổi so với kết quả ở bước số 7A).**

****

**12A) Trên router2, thực hiện lại lệnh arp và nhận xét kết quả hiển thị. Không có sự thay đổi gì**

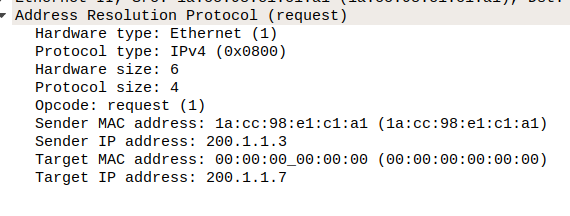
****

**13A) Trên máy thực, dùng Wireshark mở các file BT6\_router2\_A.pcap, chọn khung vật lý số 1:**

****

=> Toàn bộ khung số thứ tự 1 có kích thước 42 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?**

**=>** Trường Opcode có giá trị (Hexadecimal) là 1 và giá trị này thể hiện rằng đây là một ARP Request.

Trường Opcode cũng có thể có giá trị (Hexadecimal) là 2, thể hiện rằng đây là một ARP Reply.

**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 gửi dữ liệu là:

* Địa chỉ MAC: 1a:cc:98:e1:c1:a1
* Địa chỉ IP: 200.1.1.3

**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**

=> Địa chỉ IP và địa chỉ MAC của máy nhận dữ liệu là:

* Địa chỉ MAC: 00:00:00:00:00:00
* Địa chỉ IP: 200.1.1.7

=> Cặp địa chỉ IP và MAC của máy nhận dữ liệu là không hợp lệ, vì địa chỉ MAC được chỉ định là 00:00:00:00:00:00, đây không phải là một địa chỉ MAC hợp lệ trong mạng Ethernet. Điều này có thể là do máy tính đó không được kết nối với mạng hoặc không phản hồi yêu cầu ARP.

**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 gửi dữ liệu là 1a:cc:98:e1:c1:a1. Đây là địa chỉ MAC của máy tính gửi dữ liệu 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**

=> Địa chỉ MAC của máy nhận dữ liệu là ff:ff:ff:ff:ff:ff, đây là địa chỉ MAC broadcast, nghĩa là tất cả các máy tính trong mạng sẽ nhận được gói tin này.

=> Địa chỉ MAC của máy gửi và nhận dữ liệu đều có bit LG là 1, nghĩa là chúng là địa chỉ được cấu hình bởi chính người quản trị mạng, không phải là địa chỉ mặc định của thiết bị.

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

=> Trường Type của Header Ethernet II có giá trị là 0x0806, đây là mã số của giao thức ARP (Address Resolution Protocol), cho biết gói tin này là gói tin ARP. ARP được sử dụng để ánh xạ địa chỉ IP sang địa chỉ MAC của thiết bị trong mạng.

**B - Giao thức ARP giữa 2 thiết bị khác nhánh mạng LAN**

**7B) Trên máy ảo pc1 và router1, lần lượt dùng lệnh arp, nhận xét kết quả hiển thị.**

=> Không có gì xảy ra



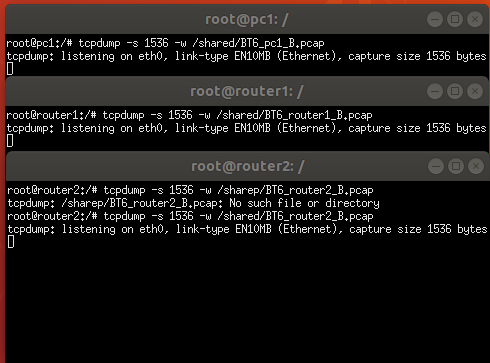


**8B) Lần lượt thực hiện lệnh tcpdump với cú pháp như sau:**

tcpdump -s 1536 -w /shared/BT6\_pc1\_B.pcap (trên máy ảo pc1)

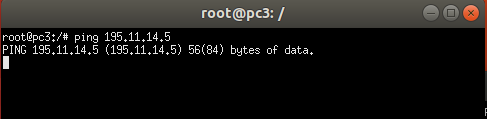
tcpdump -s 1536 -w /shared /BT6\_router1\_B.pcap (trên máy ảo router1)

tcpdump -s 1536 -w /shared /BT6\_router2\_B.pcap (trên máy ảo router2)

****

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

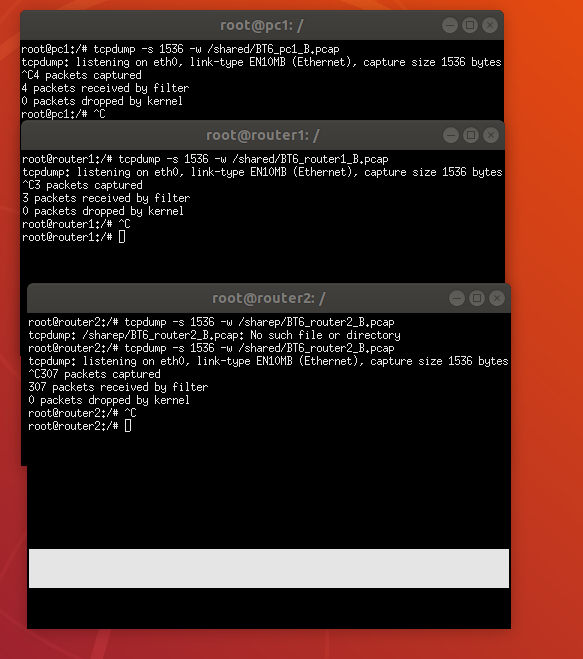
ping 195.11.14.5

****

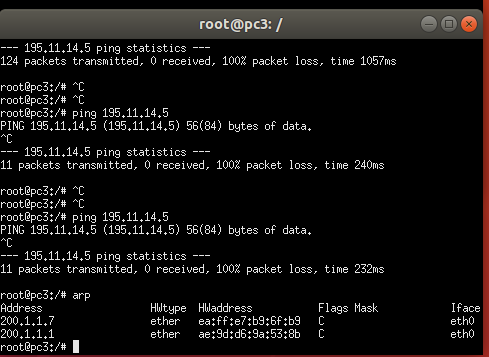
**và chờ khoảng 10 giây, sau đó dừng lệnh ping trên pc3 lại.**

****

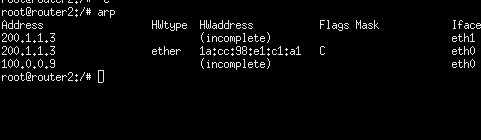
**Dừng các lệnh tcpdump trên pc1, router1 và router2.**

****

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

****

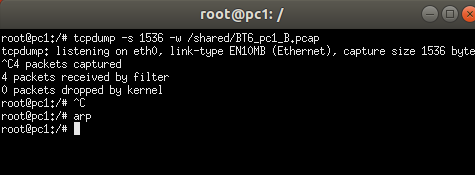
**11B) Trên router2, thực hiện lại lệnh arp và nhận xét kết quả hiển thị. Lưu ý: so sánh với 12A**

****

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

**13B) Trên pc1, thực hiện lại lệnh arp và nhận xét kết quả hiển thị. Lưu ý: so sánh**

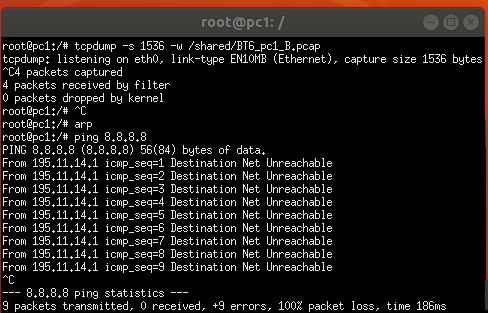
**với thông tin hiển thị của máy pc1 tại 7B**

****

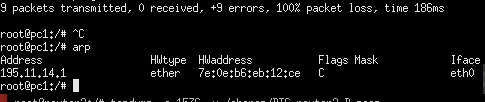
**14) Giảm tải**

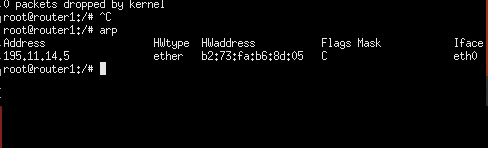
**15) Trên PC1, ping đến địa chỉ 8.8.8.8 (địa chỉ ngoài mạng ảo). Kiểm tra sự hoạt động của giao thức ARP và kết quả hiển thị trên khi dùng lệnh arp trên PC1 và Router1**

ping 8.8.8.8

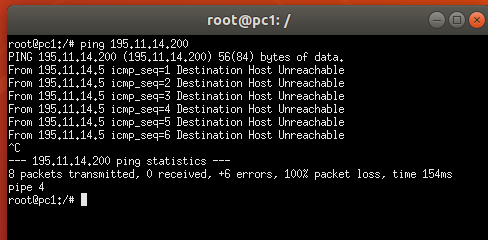
****

- Ghi nhận kết quả hiển thị khi dùng lệnh arp trên pc1 và router1.

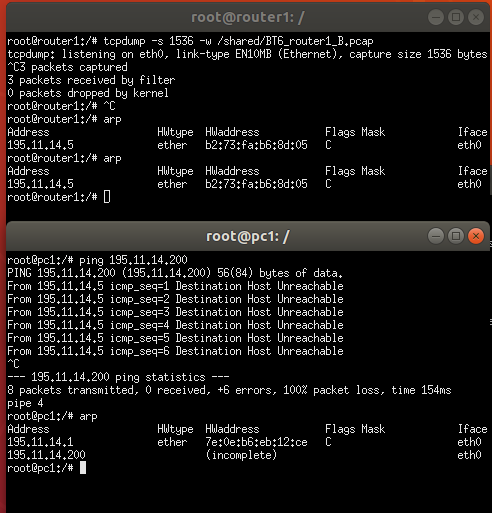




**16) Trên PC1, ping đến địa chỉ 195.11.14.200 (địa chỉ thuộc mạng ảo A nhưng không được gán cho máy tính nào cả). Kiểm tra sự hoạt động của giao thức ARP và kết quả hiển thị trên khi dùng lệnh arp trên PC1 và Router1**

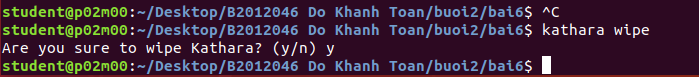
****

- Ghi nhận kết quả hiển thị khi dùng lệnh arp trên pc1 và router1.



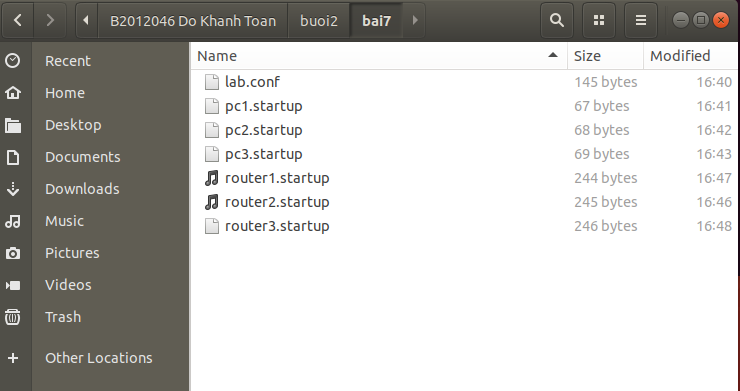
**17) Hủy mạng ảo bằng lệnh lwipe sau khi đã thực hiện xong Bài tập 6.**

kathara wipe

****

**Lap 7:**

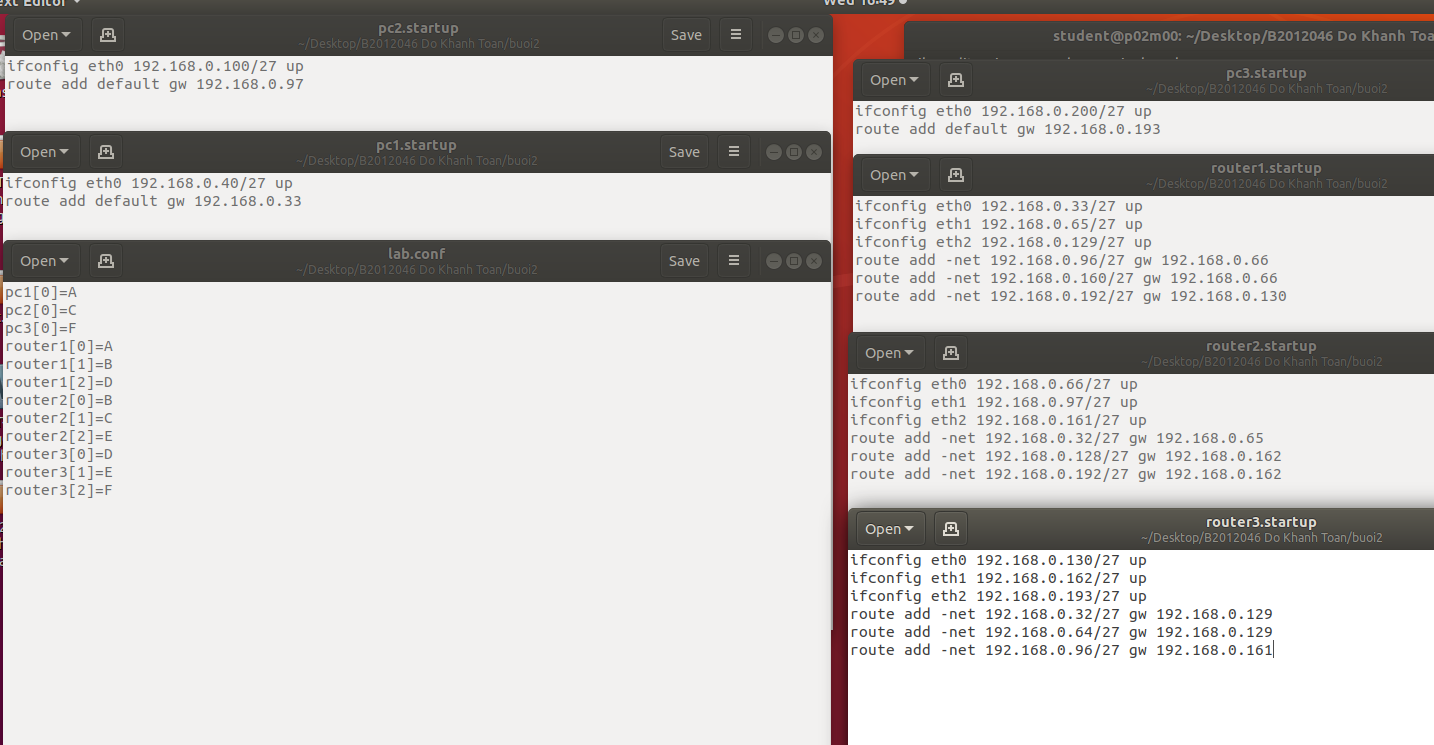
**Thư mục bai7:**

****

**3,4,5 ) Trên file lab.conf, soạn thảo nội dung mô tả hình thái mạng theo thiết kế**

**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**

**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**

=> Trên 3 câu trên được gộp vào 1 ảnh bên dưới bao gồm:  ****

**Cấu hình file conf:**

pc1[0]=A

pc2[0]=C

pc3[0]=F

router1[0]=A

router1[1]=B

router1[2]=D

router2[0]=B

router2[1]=C

router2[2]=E

router3[0]=D

router3[1]=E

router3[2]=F

**Cấu hình pc1,2,3.startup**

ifconfig eth0 192.168.0.40/27 up

route add default gw 192.168.0.33

**Cấu hình router1,2,3.startup**

ifconfig eth0 192.168.0.33/27 up

ifconfig eth1 192.168.0.65/27 up

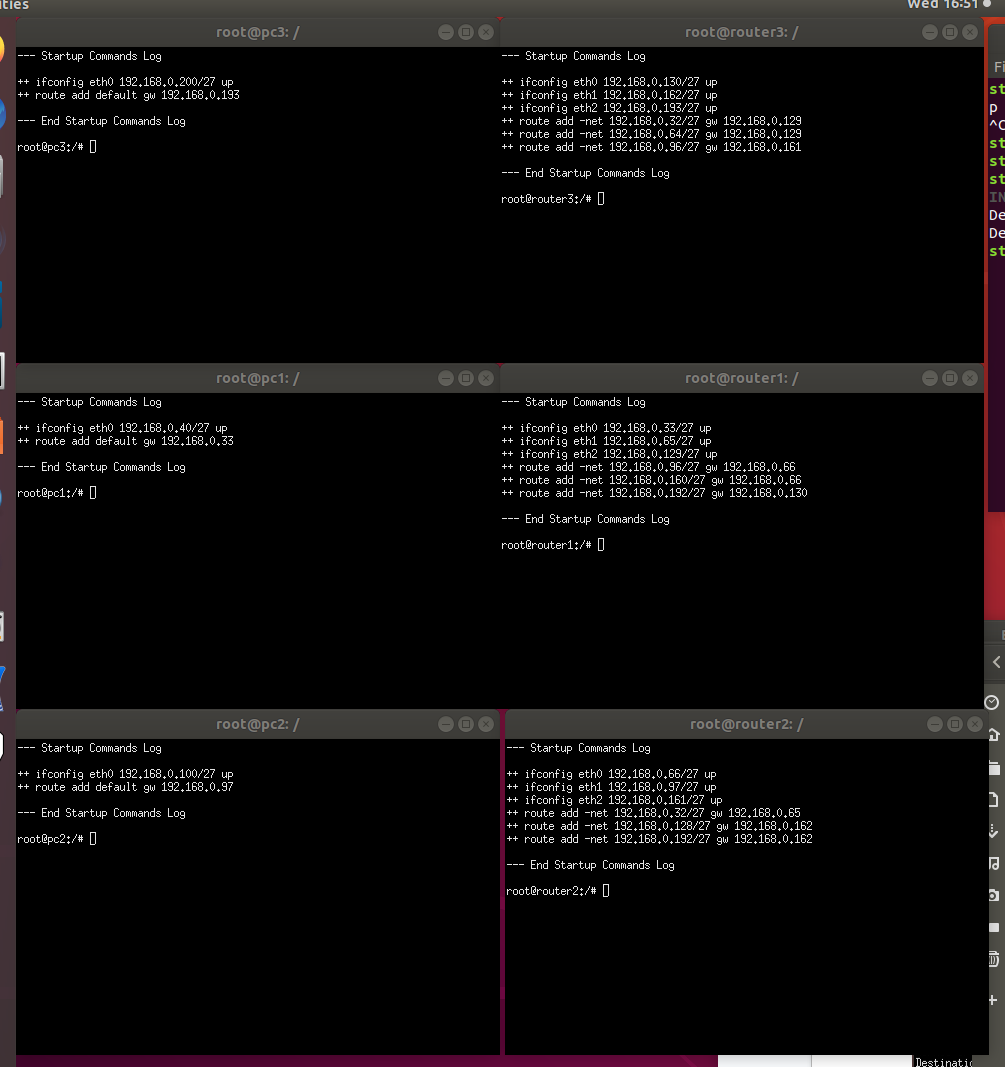
ifconfig eth2 192.168.0.129/27 up

route add -net 192.168.0.96/27 gw 192.168.0.66

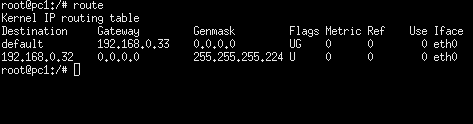
route add -net 192.168.0.160/27 gw 192.168.0.66

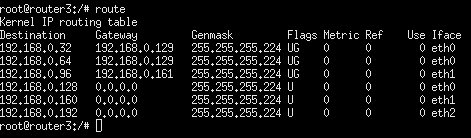
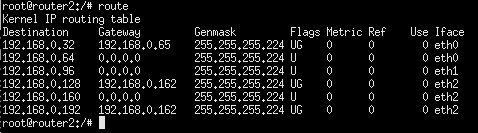
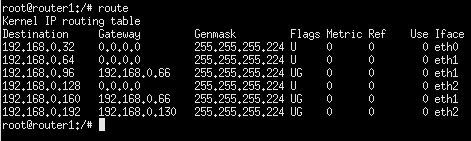
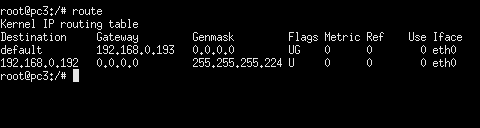
route add -net 192.168.0.192/27 gw 192.168.0.130

**6) Khởi động mạng ảo BT10. Kiểm tra bảng vạch đường (bằng lệnh route) trên từng thiết bị mạng. Kiểm tra tính liên thông giữa các máy tính PC1, PC2 và PC3 trong mạng (bằng lệnh ping)**

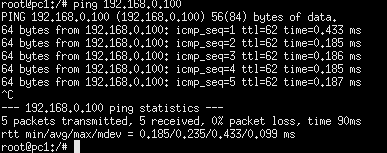
****

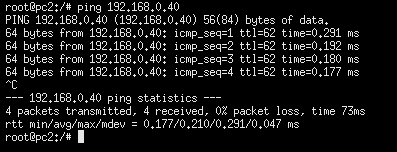
* **Kiểm tra bảng vạch đường (bằng lệnh route) trên từng thiết bị mạng.**

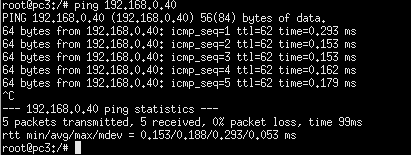
****

****

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

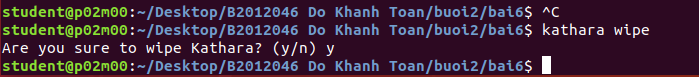
****

****

****

**7) Hủy mạng ảo bằng lệnh lwipe sau khi đã thực hiện xong Bài tập 7**

kathara wipe

****