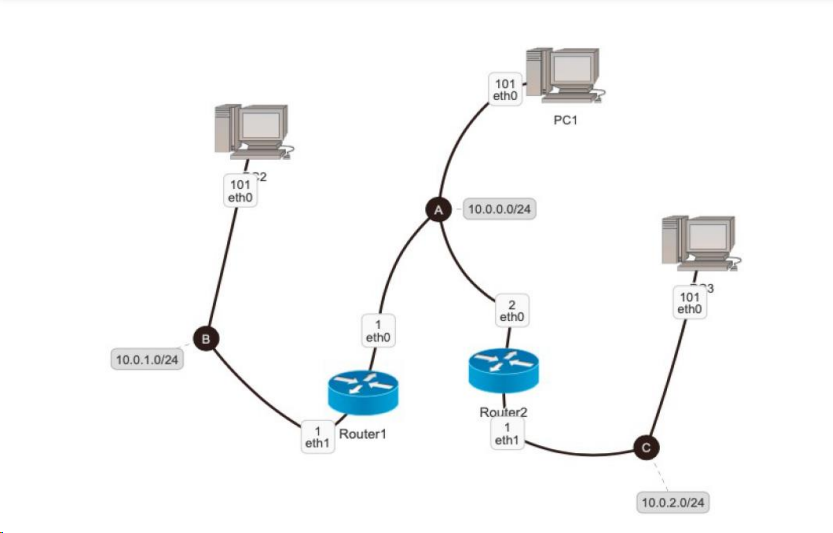
**THỰC HÀNH BUỔI 2**

**BÀI TẬP 5: Vạch đường tĩnh và gói tin ICMP**

Mục tiêu: 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 và nhận diện các thiết bị (PC, Router,..), giao diện (eth0, eth1,…) với các địa chỉ IP được gán.

- C lớp địa chỉ IP 10.0.2.0/24 là vạch đường liên mạng không phân lớp và sử dụng 3 byte cho phần nhận diện mạng. Mạng này chỉ có 2 thiết bị là pc3 và eth1 của router2

- A có địa chỉ là 10.0.0.0/24 mạng này có 3 thiết bị: pc1, card mạng eth0 của router 1 và eth0 của router2

- B có địa chỉ là 10.0.1.0/24 có 2 thiết bị: pc2 và eth1 của router1

Bước 2: Tạo cấu trúc thư mục mạng ảo (trong thư mục /home/student/CT112/buoi3/BT8) với đầy đủ các thư mục con và các file cấu hình (.startup, lab.conf) theo cấu trúc quy định của Kathará.

Bước 3: Biên soạn nội dung file lab.conf 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

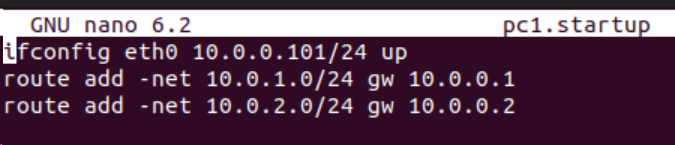


Bước 4: Biên soạn pc1.startup bao gồm thông tin vạch đường đến LAN B và C

ifconfig eth0 10.0.0.101/24 up

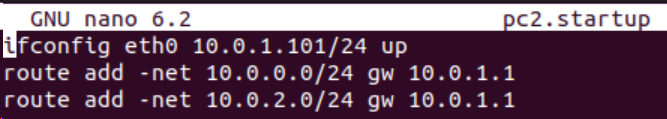
route add -net 10.0.1.0/24 gw 10.0.0.1

route add -net 10.0.2.0/24 gw 10.0.0.2

Lệnh route add -net gw cho phép thêm thông tin vạch đường theo dạng tĩnh tới 1 mạng. 

Bước 5: 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)

- pc2.startup



- pc3.startup

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 nhằm giúp cho router1 biết đường đi tới LAN C và router2 biết đường đi tới LAN B.

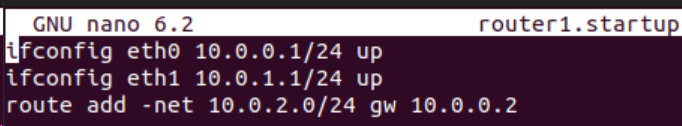
Nội dung file router1.startup như sau:

ifconfig eth0 10.0.0.1/24 up

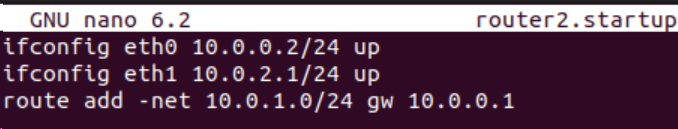
ifconfig eth1 10.0.1.1/24 up

route add -net 10.0.2.0/24 gw 10.0.0.2

- router1.startup



- router2.startup

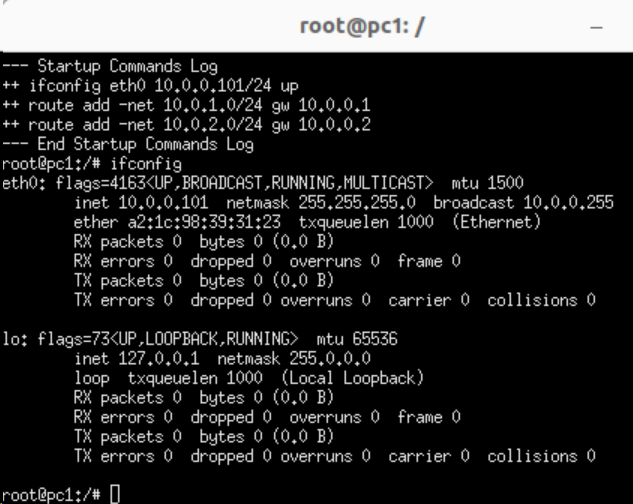


Bước 7: Khởi động mạng ảo BT8 bằng lệnh $sudo kathara lstart 

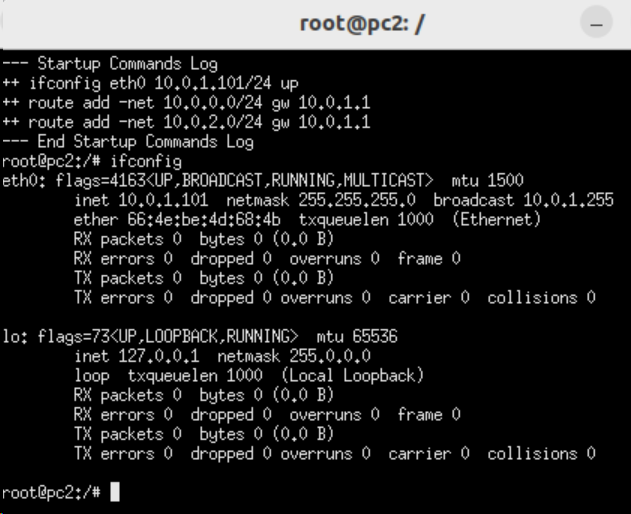
Kiểm tra bảng vạch đường (bằng lệnh route) trên từng thiết bị mạng (máy ảo). Nếu bảng vạch đường của máy ảo nào đó bị sai, thực hiện:

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

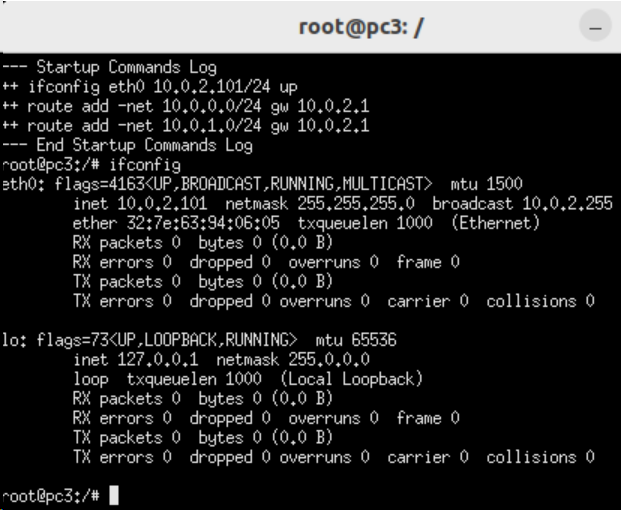
- pc1



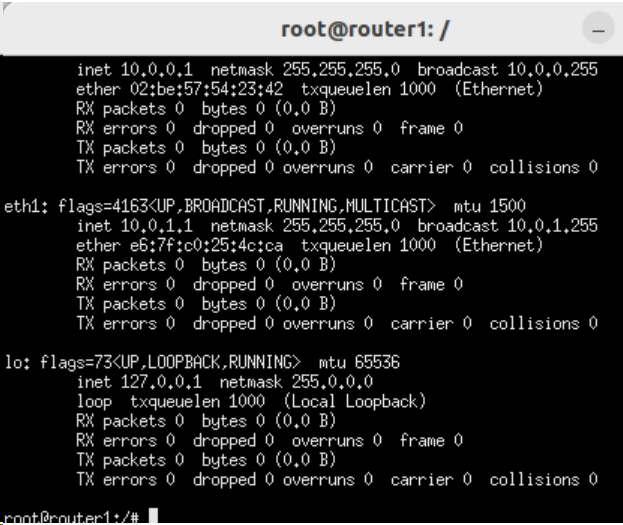
- pc2



- pc3



- router1



- router2

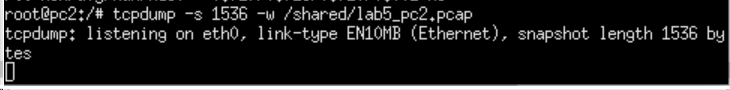


- Tắt máy ảo (kathara lclean ) và chỉnh sửa lại chỗ sai trước khi khởi động lại máy ảo (kathara lstart )

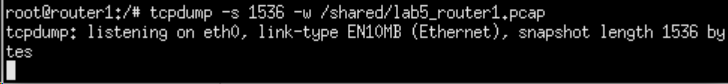
- Đôi khi, việc khởi động lại toàn bộ mạng ảo (lrestart) nên được thực hiện sau khi đã chỉnh xong lỗi sai cho thao tác cấu hình của 1 máy ảo.

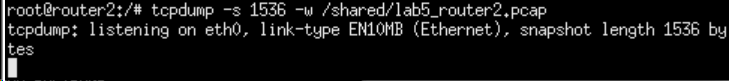
Bước 8: Trường hợp bảng vạch đường của các thiết bị đều đúng, trên pc2, router1 và router2 lần lượt thực hiện lệnh tcpdump với cú pháp như sau:

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



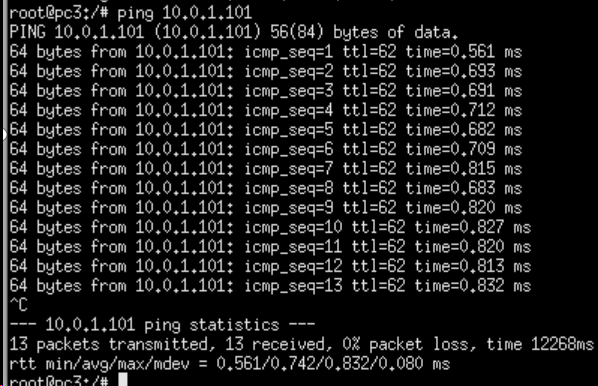
tcpdump -s 1536 -w /shared/BT8\_router1.pcap (trên máy ảo router1)



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

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

Bước 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.



Bước 10: Dừng các lệnh tcpdump trên pc2, router1 và router2 lại.

Bước 11: Trên máy thực, mở file pc2.pcap bằng Wireshark. Chọn khung vật lý (physical frame) số 6 và trả lời các câu hỏi sau đây:

- Toàn bộ khung số 6 có kích thước là bao nhiêu (Bytes)?

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

o Gói tin này sử dụng giao thức gì? Giao thức này hoạt động trên tầng nào của mô hình OSI?

o Nội dung 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: o Địa chỉ IP của máy gửi dữ liệu là bao nhiêu? Địa chỉ IP này là của máy tính nào trong mạng?

o Địa chỉ IP của máy nhận dữ liệu là bao nhiều? Địa chỉ IP này là của máy tính nào trong mạng?

o 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?

o Độ dài phần Header của thông điệp IP là bao nhiều? Phần Header bao gồm những trường (fields) nào? Mỗi trường có độ dài bao nhiêu?

o 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:

o 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?

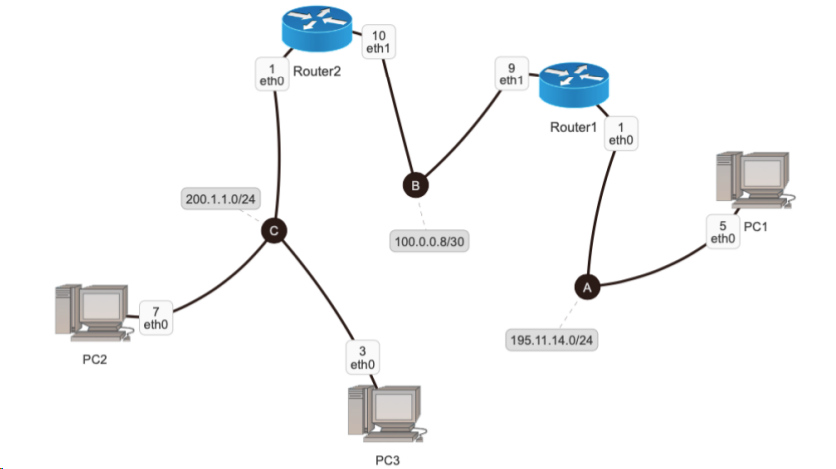
o Địa chỉ MAC của máy nhận dữ liệu là bao nhiêu? Có phải là địa chỉ MAC của máy tính có địa chỉ IP (destination) đã tìm được trong câu trên không? Nếu không, hãy lý giải và cho biết địa chỉ MAC này là của máy tính nào trong mạng?

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

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

Bước 12: Hủy mạng ảo bằng lệnh lwipe sau khi đ. thực hiện xong Bài tập 8

**BÀI TẬP 6: Vạch đường tĩnh và gói tin ARP**



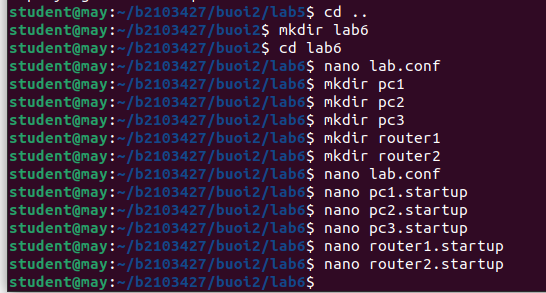
Bước 1: Quan sát mô hình mạng cần xây dựng. Nhận diện các thiết bị (PC, Router...), giao diện (eth0, eth1...) với các địa chỉ IP được gán

- Mạng A có địa chỉ là 195.11.1.0/24 có 2 thiết bị: pc1 và eth0 của router1

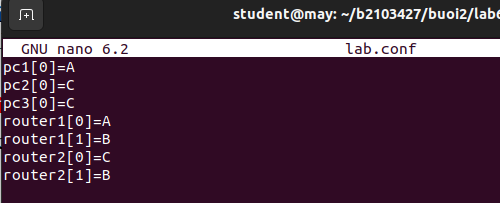
- Mạng B có địa chỉ 100.0.0.8/30 có 2 thiết bị: eth1 của router1 và eth1 của của router2

- Mạng C có địa chỉ 200.1.1.0/24 có 3 thiết bị: pc2, pc3 và eth0 của router2

Bước 2: Xây dựng cấu trúc thư mục mạng ảo (nằm dưới workspace /home/student/CT112/buoi3/BT9) với đầy đủ các thư mục con và các file cấu hình (.startup, lab.conf).

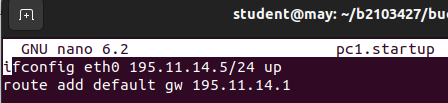


Bước 3: Trên file lab.conf, soạn thảo nội dung mô tả hình thái mạng theo thiết kế

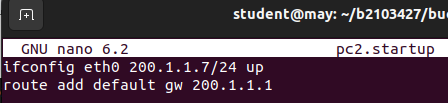


Bước 4: Trên file PC1.startup, PC2.startup và PC3.startup, thông tin vạch đường được bổ sung vào bảng vạch đường bằng lệnh route add default gw hoặc lệnh route add -net đã giới thiệu ở bài thực hành 5.xxx

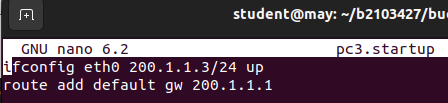
- PC1.startup



PC2.startup

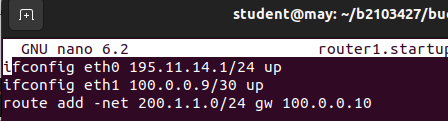


PC3.startup

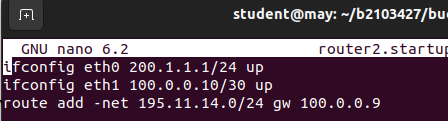


Bước 5: Trên file Router1.startup và Router2.startup cũng thực hiện bổ sung thông tin vạch đường vào bảng vạch đường sao cho Router1 biết đường đi tới LAN C và Router 2 biết đường đi tới LAN A.

- Router1.startup

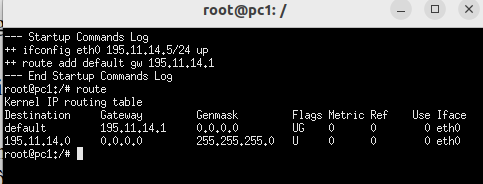


- Router2.startup

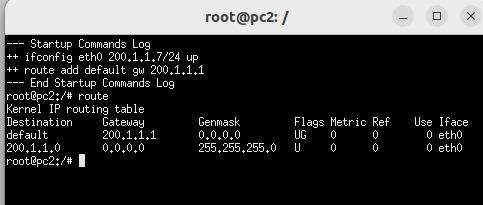


Bước 6: Khởi động mạng ảo BT9. Kiểm tra bảng vạch đường (bằng lệnh route) trên từng thiết bị mạng. Nếu bảng vạch đường của 1 thiết bị nào đó bị sai, kiểm tra lại cấu hình mạng (bằng lệnh ifconfig) của thiết bị đó. Khởi động lại thiết bị hoặc khởi động lại mạng ảo (nếu cần).

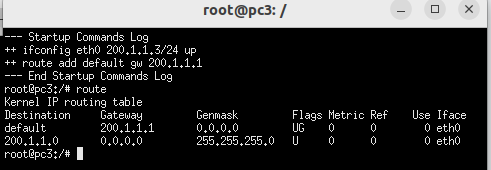
- lệnh route trên pc1



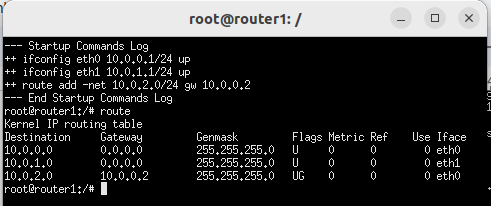
- lệnh route trên pc2



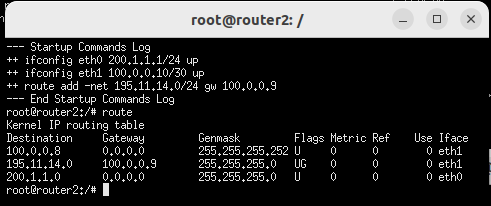
- lệnh route trên pc3



- lệnh route trên router1



- lệnh route trên router2



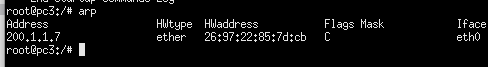
A – Giao thức ARP giữa 2 thiết bị trong cùng mạng LAN

Bước 7A: Trường hợp bảng vạch đường của các thiết bị đều đúng, trên máy ảo PC3, PC2 và Router2, lần lượt dùng lệnh arp và nhận xét kết quả hiển thị.

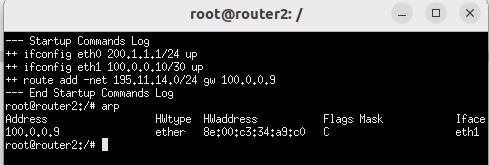
- lệnh arp trên pc2

IMG_256

- lệnh arp trên pc3

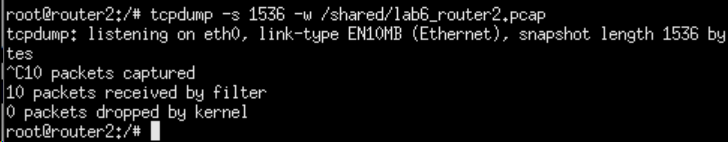


- lệnh arp trên router2



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

tcpdump -s 1536 -w/shared /BT9\_PC2.pcap trên máy ảo PC2

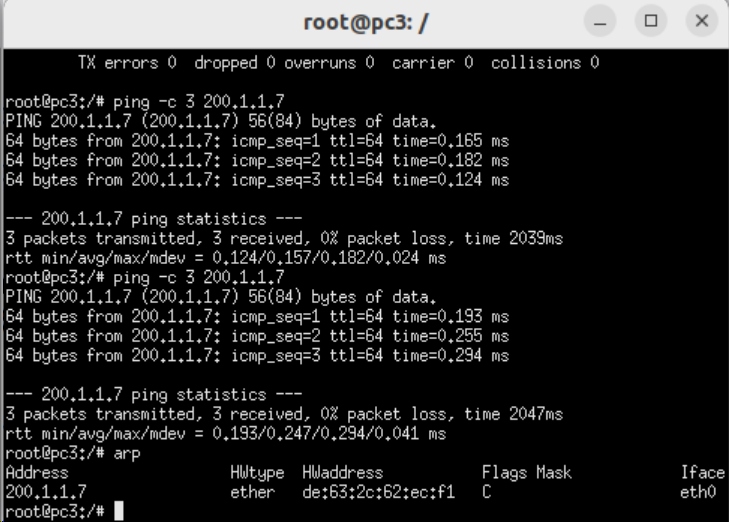


tcpdump -s 1536 -w /shared /BT9\_Router1.pcap trên máy ảo Router1

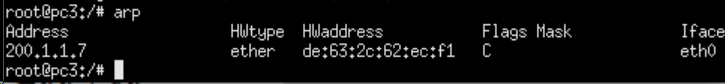
tcpdump -s 1536 -w /shared /BT9\_Router2.pcap trên máy ảo Router2



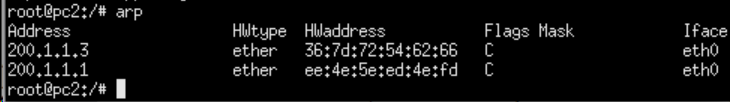
Bước 9A: Trên PC3 thực hiện lệnh ping đến PC2 (200.1.1.7) và chờ khoảng 10 giây. Sau đó dừng lệnh ping trên PC3 lại. Dừng các lệnh tcpdump trên PC2, Router1 và Router2 lại.



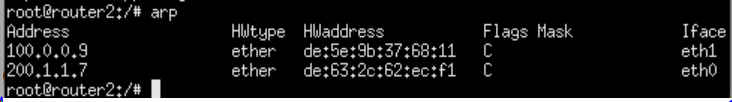
Bước 10A: Trên PC3 thực hiện lại lệnh arp và nhận xét kết quả hiển thị. Lưu ý sự thay đổi so với kết quả ở bước số 7A. Lý giải cho sự thay đổi này.



Bước 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. Lý giải cho sự thay đổi này.



Bước 12A: Trên Router2, thực hiện lại lệnh arp và nhận xét kết quả hiển thị.



Bước 13A: Trên máy thực, dùng Wireshark mở các file BT9\_Router2.pcap, chọn khung vật lý (frame) số 1

- Toàn bộ khung số 1 có kích thước là bao nhiêu (Bytes)?

- Chọn Header Address Resolution Protocol và cho biết :

o 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?

o 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? o 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:

o Địa chỉ MAC của máy gửi dữ liệu là bao nhiêu? Địa chỉ MAC này là của máy tính nào trong mạng?

o 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

o 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 và nhận xét kết quả hiển thị.

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

tcpdump -s 1536 -w /shared/BT9\_PC1.pcap trên máy ảo PC2

tcpdump -s 1536 -w /shared /BT9\_Router1.pcap trên máy ảo Router1 tcpdump -s 1536 -w /shared /BT9\_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 lại. Dừng các lệnh tcpdump trên PC1, Router1 và Router2 lại.

Bước 10B: Trên PC3 thực hiện lại lệnh arp và nhận xét kết quả hiển thị. Lưu ý: so sánh với bước số 10A.

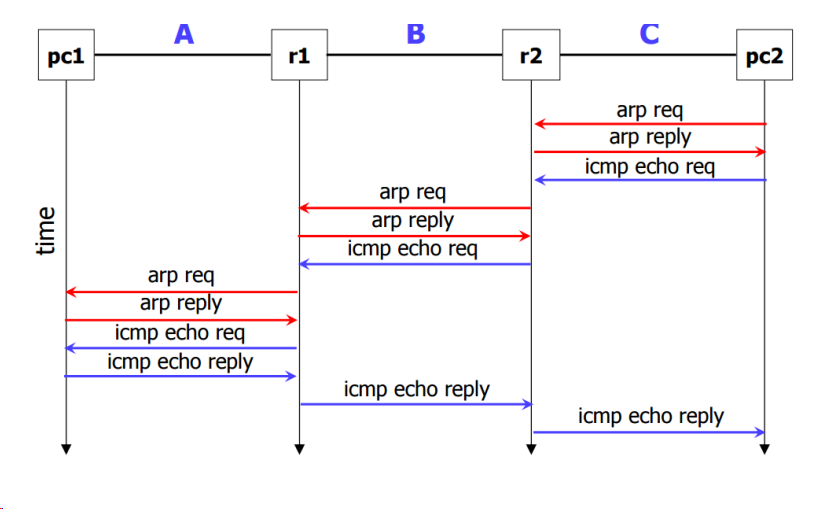
Bước 11B: Trên Router2, thực hiện lại lệnh arp và nhận xét kết quả hiển thị. Lưu ý: so sánh với bước số 12A.

Bước 12B: Trên Router1, thực hiện lại lệnh arp và nhận xét kết quả hiển thị.

Bước 13B: Trên PC1, thực hiện lại lệnh arp và nhận xét kết quả hiển thị. Lưu ý: so sánh với bước số 7B.

Bước 14B: Trên máy thực, dùng Wireshark mở các file BT9\_Router1.pcap, chọn khung vật lý (frame) số 1

- Có thể trả lời lại các câu hỏi giống như phần 13A - 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 hoặc kithara wipe sau khi đã thực hiện xong Bài tập 9